

A n a l y t i c s R e p o r t

Wireless Nation 2011: With 802.11n, Inevitability

Cutting the cord for employees and visitors is a matter of *when*, not *if*. Wi-Fi speeds now rival copper, and security advancements mean your data will be safe. There's no reason to wait, so when you're allocating those FY2011 budget dollars, think 11n.

By Grant Moerschel



A n a l y t i c s R e p o r t

T
A
B
L
E

O
F

C
O
N
T
E
N
T
S

5	About the Author
6	Executive Summary
7	Research Synopsis
8	On the Move
14	Who Makes the Rules?
15	Profile: IEEE and the Wi-Fi Alliance
17	Wide Support
22	What We Want
31	802.11n as the Game Changer
35	No Free Lunch
39	Architectural Matters
42	WLAN Vendors
46	Regulatory Compliance and WLAN Security
50	Education's Role
54	Conclusion
56	Appendix
60	Related Reports



A n a l y t i c s R e p o r t

T
A
B
L
E
O
F
C
O
N
T
E
N
T
S

- 9 Figure 1: WLAN Worries
- 11 Figure 2: Wireless Use
- 18 Figure 3: Use of 802.11
- 19 Figure 4: Impact of 802.11n Ratification on Wireless Plans
- 20 Figure 5: WLAN Predictions
- 21 Figure 6: Maintenance Timeframe for 802.11a/b/g Networks
- 22 Figure 7: Reasons for Maintaining 802.11a/b/g Networks Longer Than Three Years
- 23 Figure 8: Interest in Wireless Technologies
- 25 Figure 9: Interest in WLAN Management and Monitoring Technologies
- 27 Figure 10: Interest in Fixed-Mobile Convergence
- 29 Figure 11: VoIP Over Wi-Fi Plans
- 32 Figure 12: Barriers to Transitioning to 802.11n
- 34 Figure 13: Re-Examination of AP Locations
- 36 Figure 14: Conversion Plans
- 37 Figure 15: 802.11n Specifications
- 38 Figure 16: WLAN Integration with Wired Infrastructure
- 40 Figure 17: Controller-Based Vs. Autonomous System
- 41 Figure 18: Concerned About Bottlenecks at the WAN Controller
- 43 Figure 19: Wireless Vendors in Use
- 44 Figure 20: Most Important Vendor Evaluation Criteria
- 45 Figure 21: Regulations Impacting Wireless Deployment and Management
- 46 Figure 22: Legacy Wireless Security
- 47 Figure 23: Wireless Authentication and Encryption in Use



A n a l y t i c s R e p o r t

T A B L E O F
CONTENTS

50	Figure 24: Steps Taken to Ensure Wireless Reliability
51	Figure 25: Familiarity With Wi-Fi Alliance Specifications
56	Figure 26: Company Revenue
57	Figure 27: Company Size
58	Figure 28: Job Title
59	Figure 29: Industry

**A n a l y t i c s R e p o r t**

**Grant
Moerschel**
WaveGard



Grant Moerschel is co-founder of WaveGard, a vendor-neutral technology consulting firm. His 21 years of IT experience encompass a wide range of strategic and tactical business technology functions, including significant experience with security engineering, IT risk and vulnerability assessments, regulatory compliance assessments, wireless and wired network engineering, and wireless technology training. He has consulted for many clients in both the public and private sectors.

Grant is a co-author of the McGraw-Hill title, *Certified Wireless Security Professional (CWSP) v2 Study Guide* and the Cisco Press title, *CCSP Flash Cards and Exam Practice Pack*. He has written numerous technical articles for *InformationWeek* and courseware for (ISC)2. He holds several well-regarded IT industry certifications, including the CISSP and CWNA, and earned his BS degree from the University of Delaware.



Executive Summary

It's been a year since our first *InformationWeek Analytics* Wireless Nation report, and one thing we can say with certainty is that the industry is buzzing with activity. Worldwide, there are now more than 700 million people using 1 billion Wi-Fi devices, says Edgar Figueroa, CEO of the Wi-Fi Alliance consortium, which creates WLAN device interoperability specifications. This coming year, Figueroa predicts that the number of devices will double, to about 2 billion. That's a lot of gear. Wi-Fi technology itself made a significant leap forward late last year, when 802.11n was formally ratified; 802.11 can now claim throughput commensurate with copper-connected devices, and enhancements have been added that increase reliability. In our *InformationWeek Analytics* 2011 Wireless LAN Survey of 339 business technology professionals, the number of organizations using 802.11 WLAN technologies as a network access method for end users on a large scale, and growing it, inched up four points over last year's poll.

On the vendor side, manufacturers have been busy refining their products and pushing sales teams to make the case that Wi-Fi is now ready for prime time and that the copper cord should be cut at the access layer. As far as 802.11n products you can actually purchase, most have stated speeds of 300 Mbps, but in contrast to a year ago, 450 Mbps products are beginning to emerge in the form of high-end access points and end user device chipsets. Though mainstream products are not yet available for the 802.11n speed ceiling of 600 Mbps, expect manufacturers to get there soon. Finally, there's the role of Wi-Fi in saving carrier cellular networks from the voracious data appetites of smartphone users.

All in all, 2011 is shaping up to be an interesting year. Here's our take on what the coming months hold for IT teams charged with mobilizing, and improving the wireless user experience, for employees and guests.



A n a l y t i c s R e p o r t

Research Synopsis

Survey Name: *InformationWeek Analytics* 2011 Wireless LAN Survey

Survey Date: September 2010

Region: North America

Number of Respondents: 339

Purpose:

To determine interest in the use of WLANs and concerns about expanding use of wireless technologies in the enterprise.

Methodology:

InformationWeek Analytics surveyed business technology decision-makers at North American organizations. The survey was conducted online, and respondents were recruited via an e-mail invitation containing an embedded link to the survey. The e-mail invitation was sent to qualified *InformationWeek* subscribers as well as to registered users of the CWNPN.com (Certified Wireless Network Professional) Web community. CWNPN is self-described as the industry standard for vendor-neutral, enterprise wireless LAN certifications, and it represents IT professionals in more than 120 countries. CWNPN respondents are individuals with a specific interest in wireless technology. Many of the group's constituents have taken the time to learn the technology from the ground up and, as such, will tend to have highly informed input. We appreciate their participation in this project.

ABOUT US | *InformationWeek Analytics'* experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at awittmann@techweb.com, executive editor **Lorna Garey** at lgarey@techweb.com and research managing editor **Heather Vallis** at hvallis@techweb.com. Find all of our reports at www.analytics.informationweek.com.



Analytics Report

On the Move

Rapid growth in the number of Wi-Fi-enabled devices is a clear indicator that the technology is now mainstream—nearly a billion people can't be wrong. But are CIOs taking some of their 2011 budget increases and building robust back-end wireless networks to effectively support all this gear? Our *InformationWeek Analytics* 2011 Wireless LAN Survey of 339 business technology professionals shows that 9% are forgoing 802.11 altogether, and 15% are still evaluating; we're not quite sure what they're waiting for. On the other end of the spectrum, 39% are using 802.11 on a large scale and growing it, up from 35% last year. The remainder fall somewhere in between.

Our advice: Don't be caught napping when employees realize you're not supporting all those Wi-Fi-enabled devices in their pockets. Yes, they can get access via carrier cellular networks. But as we'll discuss in more depth, despite ongoing upgrades from current circuit-switched technologies to data-switched methods like HSPA+ and LTE, cellular bandwidth demand will continue to outstrip supply. Carriers are exploring ways to improve the user experience by seamlessly offloading some data traffic to higher-bandwidth Wi-Fi networks.

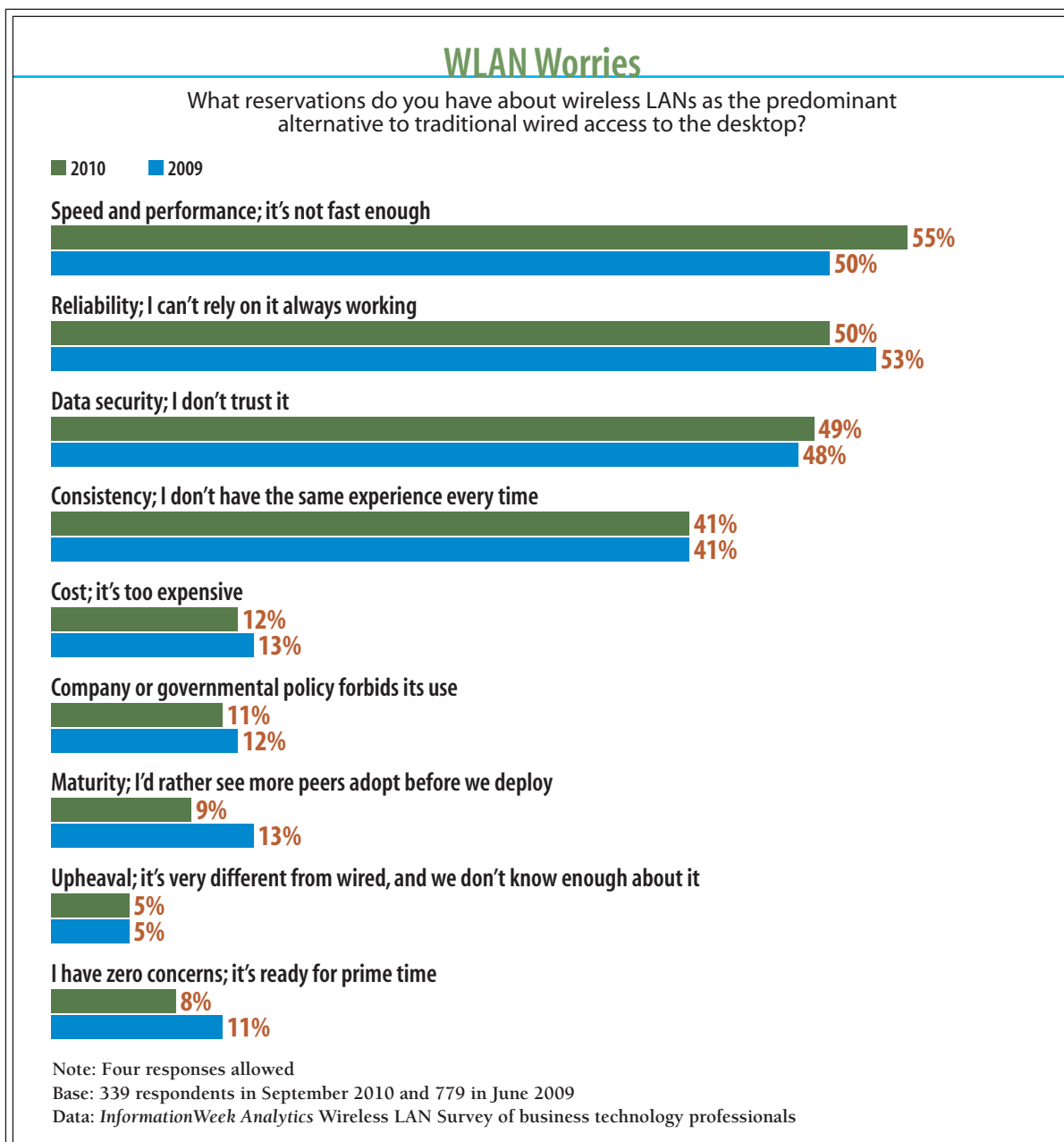
In fact, our bold statement is this: Mobility is king, and that means it's not a question of *whether* you'll go to 802.11n wireless at the access layer. It's a question of *when*. Tethered user networking as we know it, and even legacy 11a/b/g, will soon be passé for all but the most security-conscious enterprises, for four main reasons:

- 1. Performance:** Even if your 11a/b/g network is made up of quality gear and runs well, trust us, it doesn't have the capacity and reliability of 11n run in the 5 GHz spectrum. A single 802.11n access point can outpace legacy gear by five to 15 times, a major increase. When your users come complaining that the Wi-Fi network in your office is slower than what they have at home, the answer is 11n.
- 2. Obsolescence:** Walk into any wiring closet and you're bound to see a stack of teal Cisco access switches. Eventually, these will reach end of life, and you'll be looking to do a technology refresh. This is the time to closely examine alternatives to see how Wi-Fi's ROI stacks up against copper upgrades. Face it, it's costly to operate parallel access layers. Most organizations will likely pilot replacement technology and phase it in over time in lieu of rip and replace. For new construction, pervasive Wi-Fi may well be less expensive than pulling hundreds of new cables.



Analytics Report

Figure 1





Analytics Report

3. Your Users: Like it or not, employees will relentlessly push IT to support more and more wireless gadgets in the workplace. In our March *InformationWeek Analytics* 2010 Mobile Device Management and Security Survey, we asked respondents whether portable, mobile or fixed-location devices would grow as a percentage of all end user gear over the coming two years. Just 8% expect to see more desktops. The top answer, with 87%, is that mobile devices, including smartphones, will become more prevalent; 68% cited portable devices (laptops, netbooks, tablets). The reasons for this shift are many, but business leaders continue to see mobility and collaboration as good for the bottom line. Though hard dollar benefits are subjective, intuitively, they're hard to deny. The increased demand will stretch your 11a/b/g network to the limit. See #1.

4. Applications: As more applications are oriented to mobility—for example, roving health-care devices or lecture halls jammed with students running Google Docs on tablets—the 11a/b/g WLAN that was deployed for convenience will need to be more pervasive, with solid coverage throughout lest the applications fail. In environments, such as manufacturing, where legacy WLANs tend to fall short due to signal reflections and interference, 11n and MIMO may now make wireless viable.

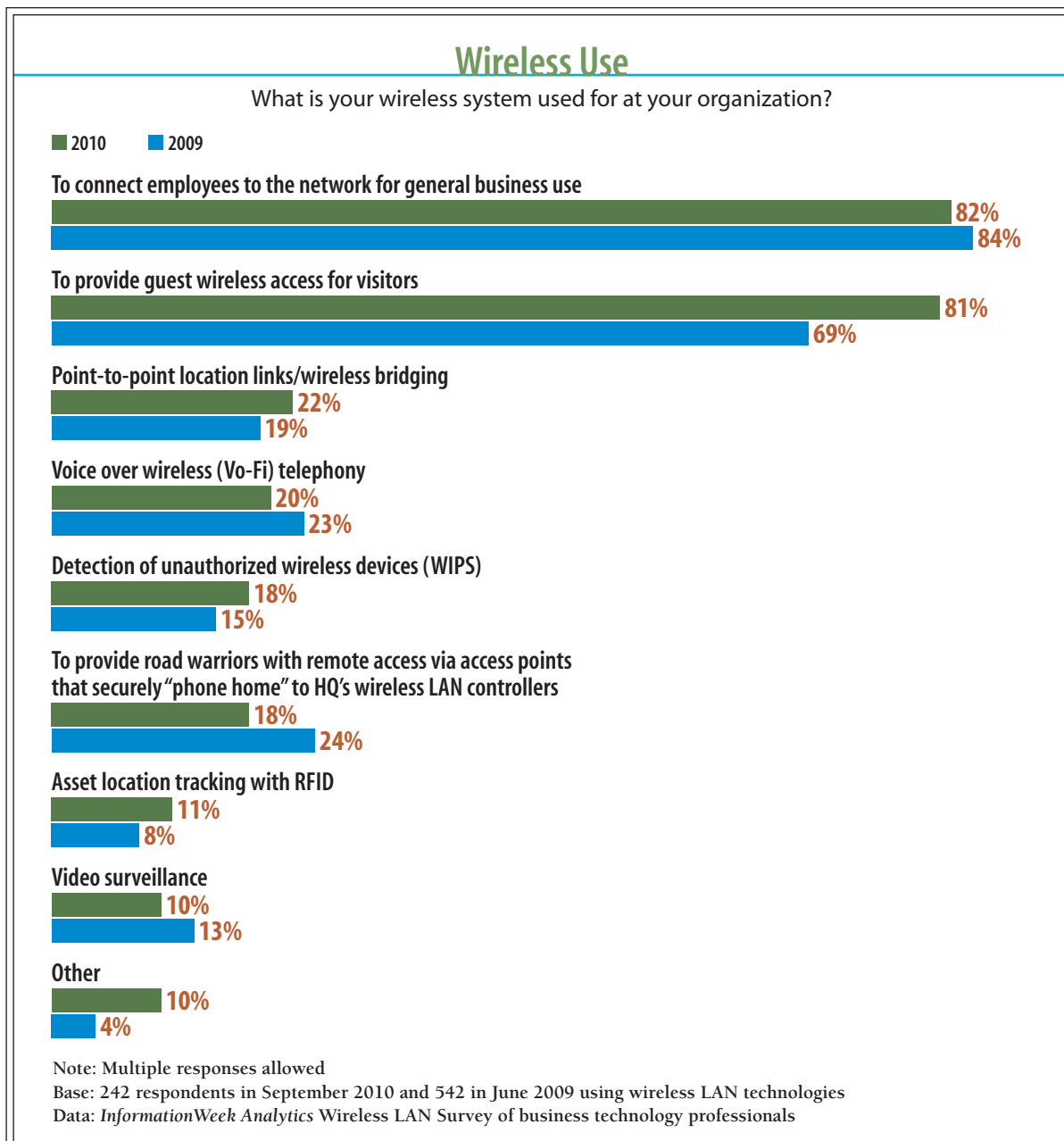
We believe that, given these catalysts, Wi-Fi will eventually supplant copper. But to get there, our survey shows that some major concerns—a few unfounded, many legitimate—need to be addressed, partly through education, partly through vendor reassurances in the form of solid products that deliver the performance and security enterprises require. As shown in Figure 1, the 339 business technology professionals responding to our survey have reservations about using 802.11 WLANs as the primary means of connecting end users to the network. Top among their worries: speed and performance (55%), reliability (50%), data security (49%), and consistency of experience (41%). These stats are strikingly similar to last year's numbers; we had expected more evolution, even given ongoing tight budgets. The data also explain why vendors are making major pushes to introduce WLAN management tools.

“Whereas WLAN security was the focus in the early part of the decade, discussions now focus much more on ways to increase reliability and performance by identifying RF interference,” says Chris Kozup, Cisco's director of marketing, mobility solutions. That explains the development effort Cisco is devoting to its CleanAir products, which are aimed at monitoring the RF environment for transmissions disruptive to radio frequencies so that they may be removed.



Analytics Report

Figure 2





Analytics Report

Amit Sinha, fellow and chief technologist for WLAN and security at Motorola Solutions, says that at the beginning of the sales process, CIOs are often biased against WLANs because of poor past experiences and may simply view wireless as a convenience mechanism, outside of and apart from the core infrastructure. Sinha says that when IT groups take the time to learn about built-in mechanisms designed to enhance reliability and consistency, tools that maybe didn't exist just a few years back, they come to understand that 11n is indeed a wired alternative. But leadership is often still most interested in the bottom line, asking, "What's this going to cost us?"

Wireless vendors must overcome these concerns with hard data, delivered in a concise way—and free from flights of fancy. When making the case for upgrading or expanding the WLAN, IT and vendors alike need to show that Wi-Fi will contribute to the bottom line by both untethering employees (hard to quantify) and by reducing hard-dollar capital and operational expenses (capex/opex) over, say, a five-year timeline. For example, Motorola is able to make a highly detailed and compelling dollars-and-cents argument down to a cost per covered square foot that will get any CFO excited. In a similar vein, Aruba Networks, also a WLAN market leader, seconds this notion with its "Network Rightsizing" models that show how infrastructure costs can be reduced by placing emphasis on RF as the transmission medium instead of installing excessive copper ports. It's up to you, the educated buyer, to decide whether these vendor models are plausible—and some are—or simply optimistic fluff.

Competition is fierce, and vendors will do what it takes to win your heart and business. But beware the sweet talk, especially when it comes to ROI. We maintain that some costs are indeed measurable, whereas others are always going to be subjective. When directly comparing several candidate WLANs, or perhaps a WLAN vs. a new wired system, there are some specific costs to keep in mind; we'll go into more depth on these technologies later, but at a minimum consider:

Capital expenses for WLAN planning and acquisition:

- **Intended use requirements:** What's the purpose of the WLAN? Is it for high-user-density or time-sensitive apps (more gear) or casual use (less gear)?
- **Coverage planning:** Where are the best AP locations for us based on the intended use?
- **Design:** What will the new WLAN infrastructure look like, and how will it integrate with our core network?



Analytics Report

- **Security:** What system changes or additions will be needed at the core in order to use enterprise-grade authentication and encryption?
- **Power:** If you don't have power over Ethernet for APs, you'll need to invest. If you already have PoE, do you need to upgrade it to the newer 802.11at, or will your new 11n WLAN platform adapt well enough to the older PoE standard?
- **Infrastructure bill of materials:** How many access points are needed? How many controllers, if any? This depends on the chosen vendor's architecture. What are the license acquisition costs for various WLAN functions, such as firewalling, IPS and mesh? Some vendors nickel and dime you based on the functions you need, others don't. Since 11n APs use gigabit copper for backhaul, will upgrades be necessary to the remaining access switches that lead to the core?
- **Client station bill of materials:** Will your current devices support the new infrastructure, or are new network cards needed? How much will retrofits cost?
- **Installation:** What's the cost to pull wires to AP locations and to hang APs?
- **System configuration:** Who will configure and tune the new WLAN?
- **Tools:** What additional hardware and software utilities are needed for management?

Operational expenses for WLAN support:

- What are the **ongoing hardware support** costs? Ongoing WLAN function license costs? Technical support costs?
- Will there be any savings or increases for **personnel to support** the WLAN?
- Will you need **consultants**?
- What additional **education** is needed?
- Will vendor features permit middle-of-the-night **proactive self-testing** to spot problems and reduce the number of "truck rolls?"



Analytics Report

- Will the WLAN be able to temporarily **self-heal** (if an AP goes bad) so that users can continue to work?

If vendor cost models introduce benefits that are difficult to quantify, be aware of their effect on the overall equation. How does one truly measure increased productivity due to mobility? And watch for unrealistic assumptions. When models start by claiming you can reduce your copper ports from four per user to near zero, yes, you will indeed save money. But do any of your buildings really have 600 ports (25 switches with 24 ports each) for 150 people? Yeah, we didn't think so.

As the industry matures, it will be easier to make the case on both the technology and the money sides. Yes, 11n is fast. Yes, it's reliable. Yes, it's secure and cost effective. And yes, your people will use it, happily.

"We all went through this with cell phones," says Motorola's Sinha. "But now everyone has a cell phone. Things are changing, especially as these digital natives—people who grew up with the technology—become an ever-larger share of the workforce. Mobility will be the expected norm."

We'd add a caveat that, to realize these benefits, organizations must understand what they're buying and all the pieces required to make it a success, including the training or acquisition of knowledgeable talent. Read on for details.

Who Makes the Rules?

InformationWeek and *Network Computing* have long been critical of the state of technology standards; lately, IPv6, HTML 5, open cloud standards and transport for e-health data are hot-button issues. But we have to admit that wireless infrastructure device, client and third-party application vendors, and other manufacturers of WLAN gear, have largely escaped being painted with the standards scofflaw brush, and enterprises seem to be giving credit where it's due. This year, when we asked poll respondents using WLAN technologies about their top product evaluation criteria, ability to integrate wired and wireless networks came in at No. 12 out of 16 possible choices, 20 points behind capital costs and just above built-in RF tools. Recognition goes largely to the IEEE and the Wi-Fi Alliance, which we profile in depth, next page. The Wi-Fi Alliance develops testbeds for ensuring vendor products adhere to interoperability specifica-



Analytics Report

tions. Curiously, Wi-Fi Certification comes in dead last among vendor criteria, which is perhaps testament to the fact that the Alliance's methods are effective and somewhat transparent to those who operate Wi-Fi networks.

Manufacturers rarely move faster than the Wi-Fi Alliance and its certification programs, because if they do, wireless clients—and their feature sets—risk not being compatible with

Profile: IEEE and the Wi-Fi Alliance

The IEEE (www.ieee.org) comprises engineers, scientists and students, often working in academia or for manufacturers. The IEEE describes itself as “a leading authority on areas ranging from aerospace systems, computers and telecommunications to biomedical engineering, electric power and consumer electronics, among others.” IEEE working groups create technology standards used around the globe. In the case of 802.11, the IEEE has defined the data communication protocols for Layers 1 and 2 of the OSI model. The 802.11 specification was initially ratified in 1997. It was amended in September 2009 with 802.11n for high-throughput wireless.

The Wi-Fi Alliance (www.wi-fi.org) is a nonprofit industry trade association comprising several hundred member companies interested in promoting and selling WLAN components. One of the Wi-Fi Alliance's main purposes is to create wireless technology specifications that mirror many, but not always all, parts of the IEEE standards. Additionally, the organization tests products based on these specifications to ensure that they interoperate. Manufacturers that create products to these specifications usually submit them to the Alliance for independent laboratory interoperability testing and certification. Once a product is certified, the manufacturer is permitted to use the “Wi-Fi Certified” logo on the packaging. Certified products, even from different manufacturers, should be able to interoperate. For example, Wi-Fi Alliance-tested wireless adapters that are certified for 802.11n will work with access points also certified to the same specification.

Current Wi-Fi certification programs include:

- > **Wi-Fi 802.11a/b/g certification:** Required by CTIA for Wi-Fi enabled handsets seeking CTIA certification.
- > **Wi-Fi Certified:** 802.11n certification.
- > **Wi-Fi Wireless Protected Access (WPA and WPA2):** Certification for highly secure Layer 2 encryption for smaller personal and larger enterprise implementations.
- > **Extensible Authentication Protocol (EAP):** Certification for seven (and counting) advanced authentication methods.
- > **Wi-Fi Multimedia (WMM):** Certification for prioritization of data to benefit time-sensitive applications.
- > **WMM Power Save:** Certification for conserving portable-unit battery life.
- > **Wi-Fi Protected Setup (WPS):** Certification for easy-to-use preshared key security.
- > **Voice - Personal:** Certification for ensuring single-AP voice communications that meet minimum standards for voice call quality.
- > **CWG-RF:** Converged Wireless Group RF is a test plan jointly developed by the Alliance and the CTIA for devices featuring both Wi-Fi and cellular technology. The spec is aimed at giving carriers and handset manufacturers consistent device performance metrics for any tested product so that network performance can be accurately predicted.



A n a l y t i c s R e p o r t

infrastructure devices. Thus, the Alliance plays a significant role in setting the manufacturing pace for certain features. Consider the IEEE 802.11r and 802.11k standards, which help define how wireless devices on the move quickly and elegantly transition, or “roam,” from one wireless access point to another—a highly important function, especially for time-sensitive applications like voice and video. Though these amendments were ratified in 2008, they are not yet implemented in vendor products because the Wi-Fi Alliance specification that addresses 11r and 11k has not been finalized. Last year, we said that the Alliance’s Voice-Enterprise certification would arrive in mid 2010, but it’s still not done, and the latest buzz has it slated for Q1 2011.

Kelly Davis-Felner, marketing director at the Wi-Fi Alliance, says her organization, which is comprised primarily of manufacturers, promotes the features *it* feels need to be made available using a one-member, one-vote system. Thus, the technologies that hit the marketplace, and the timing thereof, are really not up to individual vendors, but rather the Alliance in aggregate.

Don’t get us wrong—the Alliance is making progress in its various certification programs. Here are three notable technologies coming soon to a product near you.

- **Wi-Fi Direct**, launched in October, enables connections among participating devices for activities such as sharing, printing, video display or synching. It can operate in peer mode or via an enterprise AP at up to 250 Mbps at a range of 200 meters. WFD adds wireless conveniences via the corporate network for visitors or employees without sacrificing overall enterprise security.
- **Protect management frames**, due in Q1 2011, will be rolled into the WPA2 security specification. When implemented, the technology will permit stations to verify the authenticity of Wi-Fi “housekeeping” communications to prevent rogue transmissions that disrupt an RF environment.
- **Voice-Enterprise certification**, due in 2011, addresses data prioritization, bandwidth management, client load balancing across APs, elegant and quick transitions among APs, security, and battery life controls in multi-AP environments.

These advances notwithstanding, a lack of speedy movement sometimes frustrates technologists and individual manufacturers, but you can’t argue with the interoperability results. While func-



Analytics Report

tionality is sometimes released outside of the Wi-Fi Alliance's aegis, most technologies that are introduced into the market in this manner are single-sided, meaning that they work on the infrastructure without the participation of the client computer. One example is ClientLink, Cisco's foray into proprietary beamforming (a transmission technique). Though there is a standards-based beamforming spec under consideration by the Wi-Fi Alliance, Cisco decided not to wait. We know that some IT pros are willing to trade openness for a proprietary functionality advantage, but our recommendation is to ensure that any products you're considering are compliant with Wi-Fi Alliance certification programs. Systems that don't have Wi-Fi product certifications will likely lock you in and may cost more in the long run.

To see which vendor products support which Wi-Fi Alliance capabilities and specifications, go to www.wi-fi.org/search_products.php?advanced=1&en.

Wide Support

We're again pleased at the diverse voices represented in our wireless LAN survey—our data provides a nice cross section of the state of wireless as a whole. As illustrated by figures 26 through 29 in the appendix, page 56, our 339 participants hail from a wide array of industries. More than 50% are spread across manufacturing, healthcare, education, government and financial services. As in our previous survey, about one-third have revenue under \$50 million, while one-third earn \$50 million to \$5 billion; the balance have more than \$5 billion in revenue, are government/nonprofits or decline to say.

WLANs are growing in popularity because of the sheer number of portable and mobile devices that are coming to market. There is a fine line between the definition of portable and mobile:

Portable implies that the device can be moved from place to place, but computing usually does not happen during movement; **mobile** on the other hand implies that the user may be operating the device while on the go. Laptops are the No. 1 portable device type for convenience computing. Likewise, mobile devices such as wireless voice-over-IP (Vo-Wi-Fi or Vo-Fi) handsets and smartphones with built-in Wi-Fi are everywhere.

And don't forget about the onslaught of pad and slate devices. Apple has shown huge success despite early skepticism, and other vendors, including RIM and Samsung, are pushing their own visions.

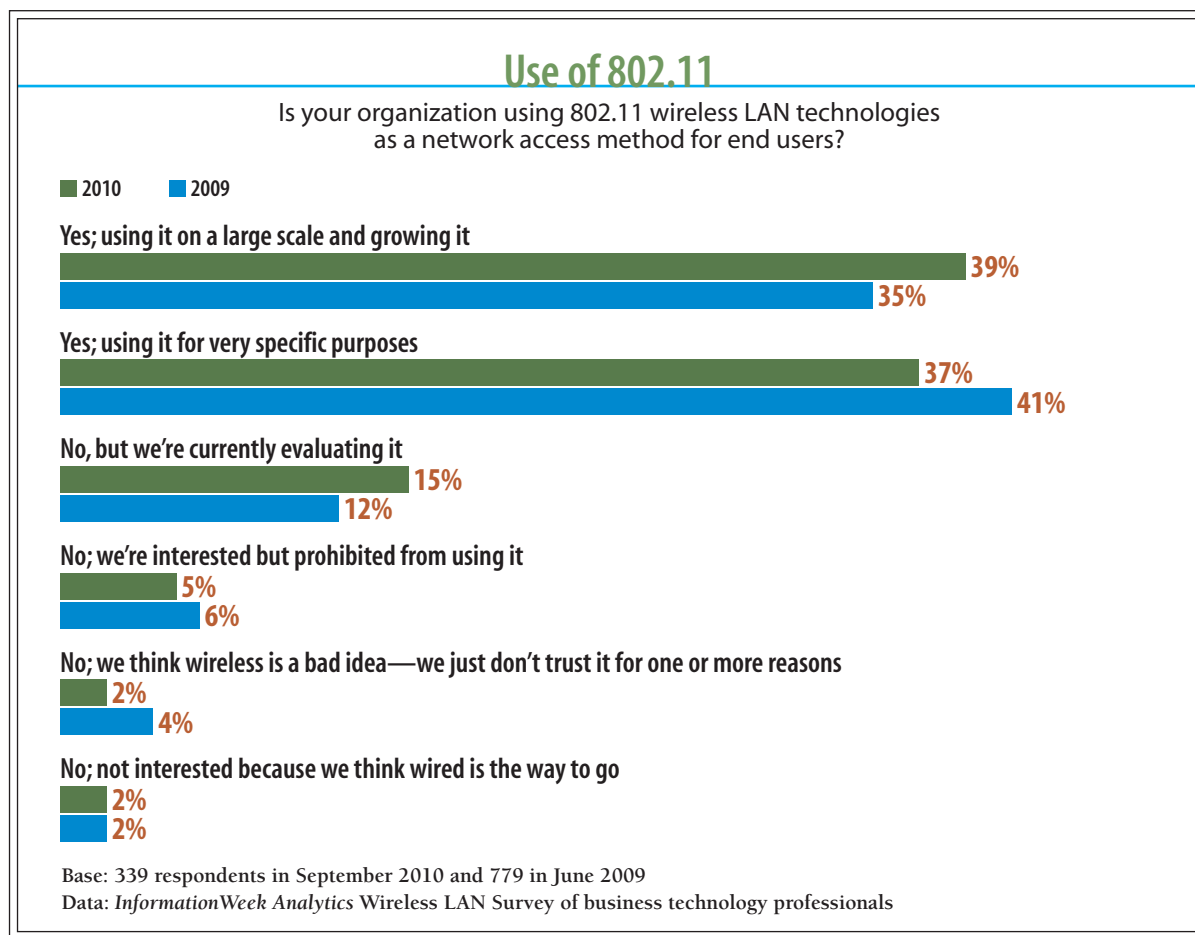


Analytics Report

It's obvious that this mobile wireless device explosion—remember, the Wi-Fi Alliance expects device numbers to double this year, and our data backs that up—demands well-designed, robust WLANs to provide reliable connectivity. Otherwise, the user experience will be poor, leading to increases in network support operational costs and an overall decrease in productivity. We'll discuss the relationship between 3/4G and Wi-Fi shortly.

Figure 3, below, shows respondents' continued high interest in using wireless technologies as an access method for connecting end users to the network, with 76% using 802.11, and 39% of those growing the wireless infrastructure. These numbers are very close to last year's survey results.

Figure 3



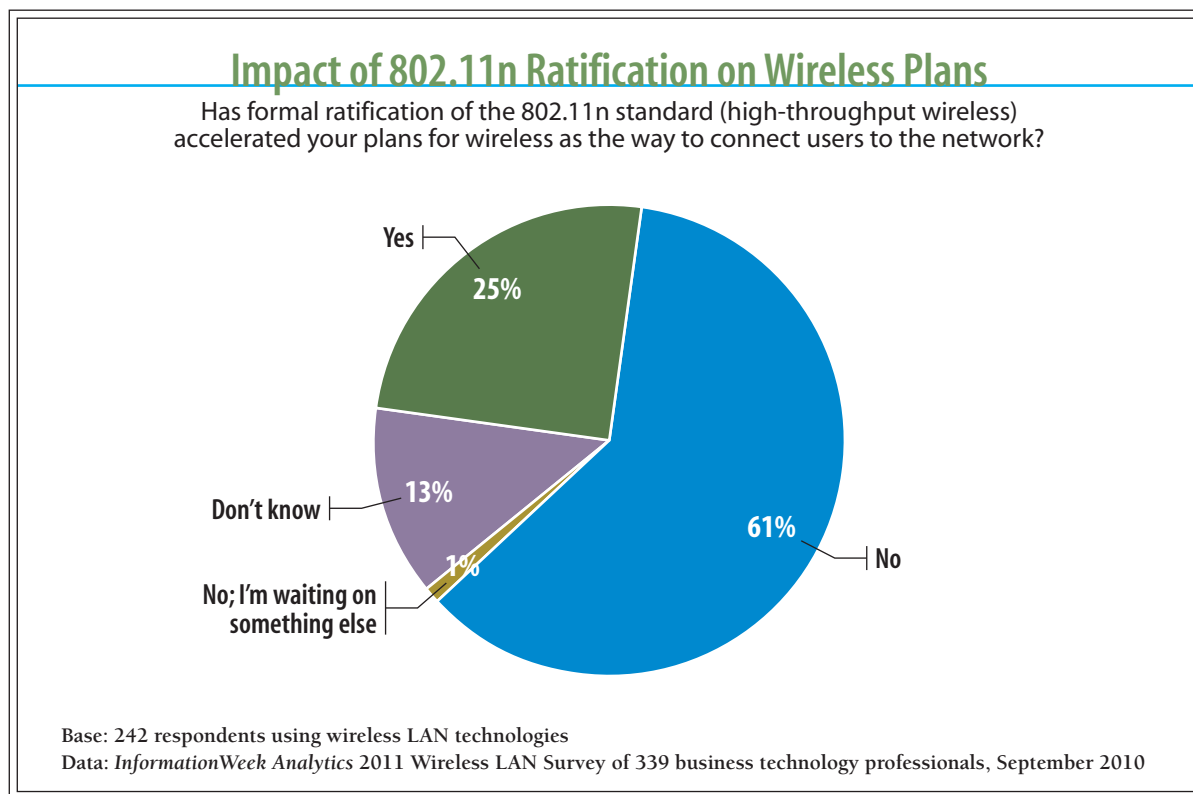


Analytics Report

A small percentage of respondents, 2%, say they think that wireless is a bad idea for one reason or another. In our experience, this is often due to concerns over security or robustness, but as mentioned, the ball's in the candidate vendor's court to make the case that this isn't necessarily so. Five percent of respondents are interested in wireless but are prohibited from using it. Often, this is because of compliance and security policies, as with government agencies that forbid WLANs due to the sensitivity of information travelling over the network.

One of our more interesting data points indicates that last year's ratification of 802.11n will *not* accelerate plans to use wireless as the primary way to connect users to the network. Almost two-thirds of respondents answered this way, which frankly surprises us. Though 802.11n is no panacea, it certainly is a big jump forward compared with 802.11a/b/g. The response can be interpreted in many ways, but it likely leads back to the top concerns cited in Figure 1: speed, reliability, security and consistency, as well as continued anemic IT budgets.

Figure 4



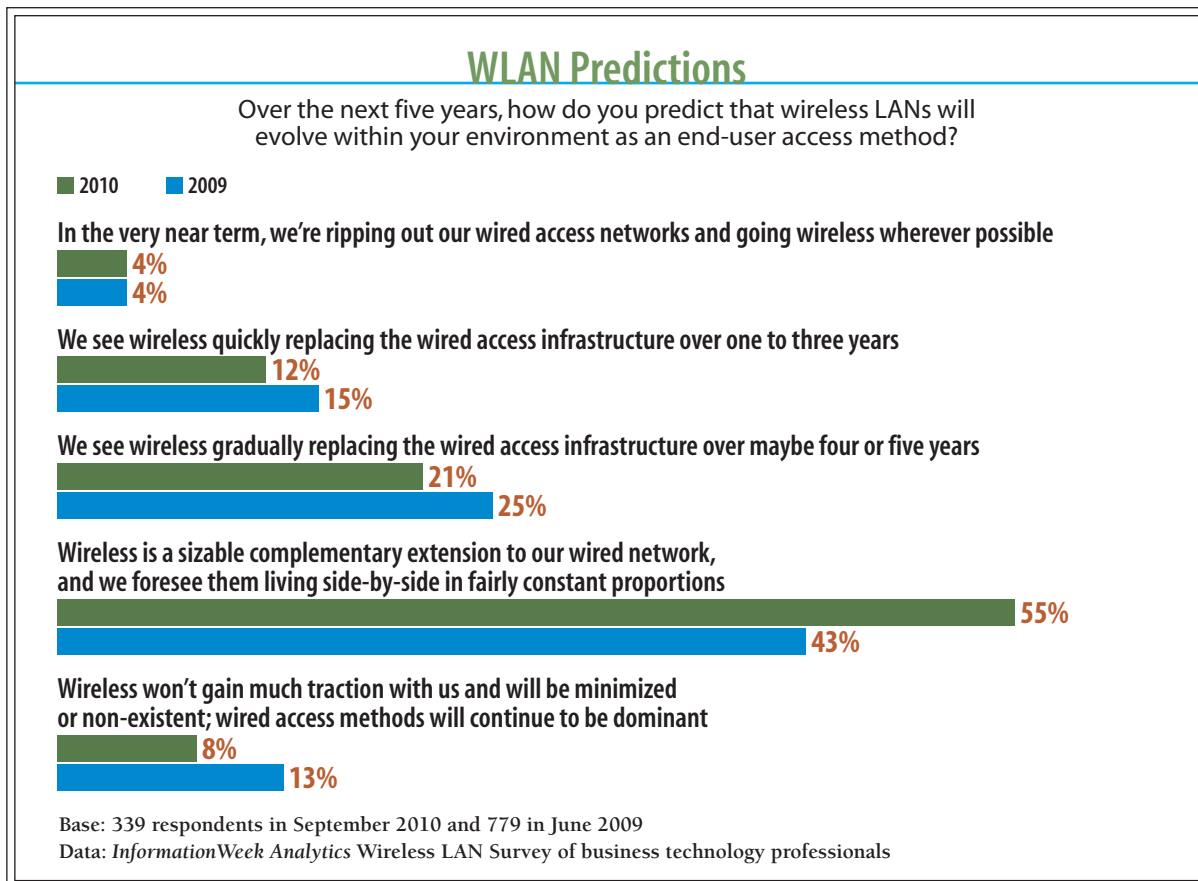


Analytics Report

When money is tight, is the WLAN a priority? Seemingly not. So it's fortunate that our *InformationWeek Analytics Outlook 2011* survey shows that IT budgets are set to recover somewhat; 55% of the more than 550 respondents to that poll say IT spending will rise next year compared with this year. Just 19% will see reductions.

So then the question is, How do respondents see WLANs evolving over the next five years as an end user access method? Figure 5, below, shows that connectivity innovators, 16%, are going full steam ahead and removing wired LANs altogether within three years. An additional 21% see WLANs more gradually replacing wired networks as the end user access method of choice. The top response, with 55%, is that wired and wireless networks will live side by side in fairly constant proportions.

Figure 5



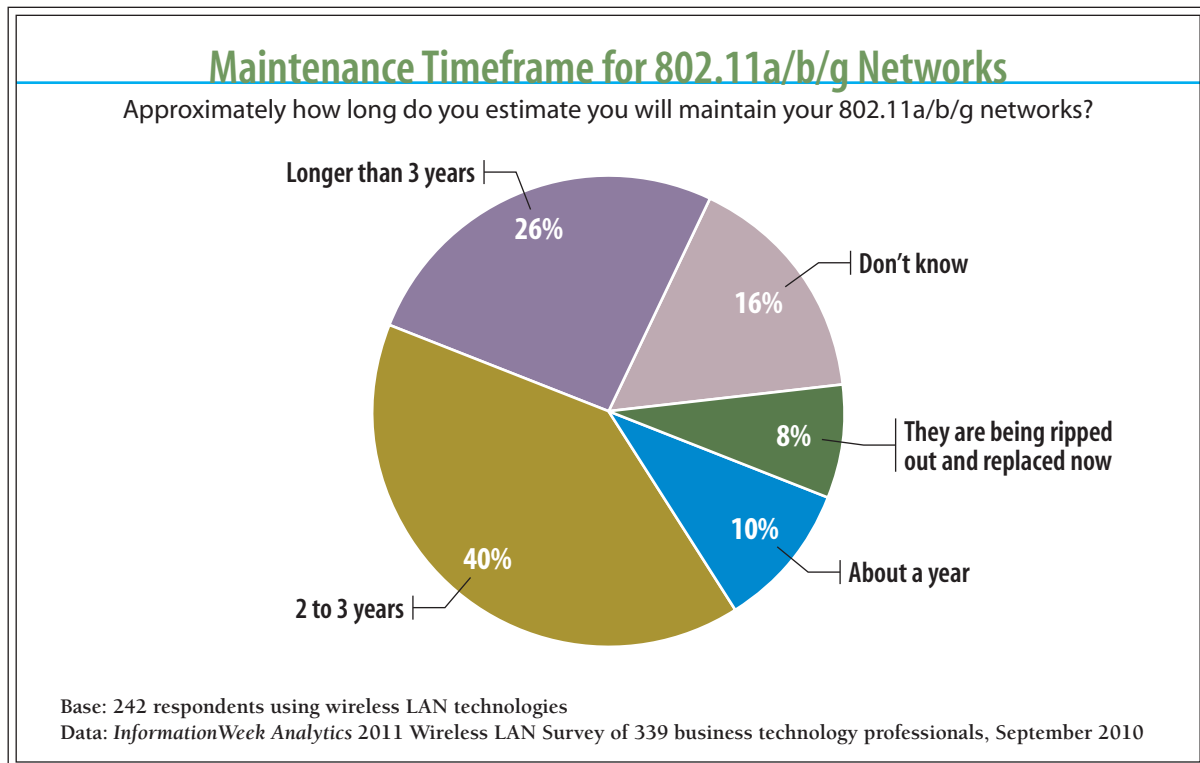


Analytics Report

For those moving forward with wireless, a big question is how long they will support legacy 802.11a/b/g gear. Our survey suggests that within three years, we'll see these older technologies marginalized in favor of 802.11n devices. This is important since a large portion of new products being certified by the Wi-Fi Alliance are 11n-centric and need an 11n infrastructure to fly their highest. Davis-Felner estimates that 59% of Wi-Fi products sold in 2010 will have 11n capability, with this number moving to 95% by 2013. She also contributes the following view of 802.11n's first full year as a standard and the Alliance's minting of the Certified n spec:

- Enterprise-grade product lines saw 157 infrastructure devices and 115 access points certified.
- Voice handsets are shifting to next-generation Wi-Fi, with 127 phones certified.
- Digital home products saw 251 new devices certified.
- For dual-band products, operating in both 2.4 GHz and 5 GHz, 584 new devices were certified.

Figure 6





Analytics Report

We asked those planning to maintain a/b/g networks longer than three years, Why? Though this time span starts to get into crystal ball territory, especially when we're talking technology, the 62 respondents here cite as the top reasons budget constraints and that a/b/g is just fine for their needs. We'll be interested to see if that holds true.

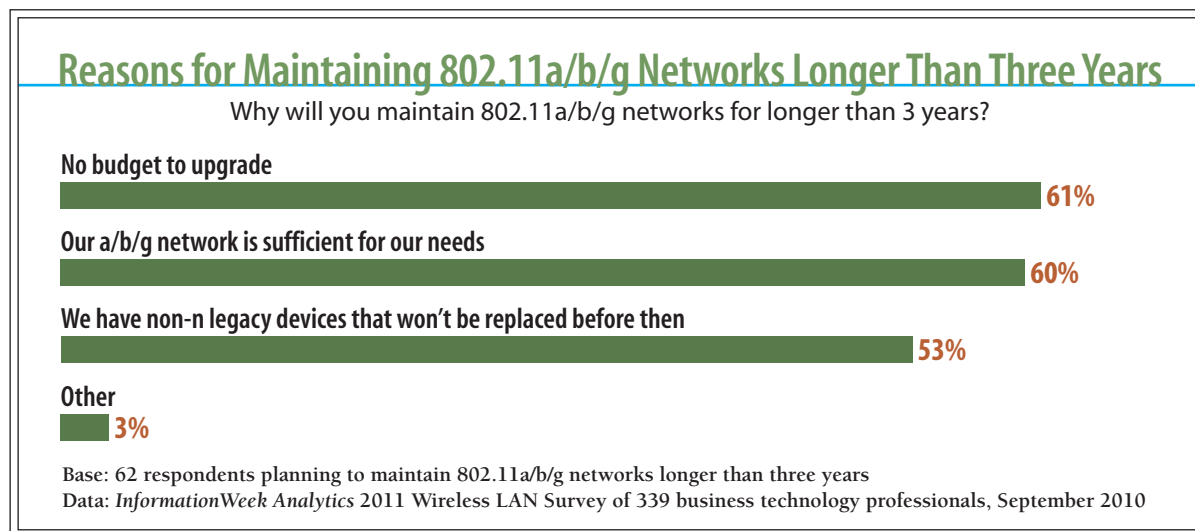
What We Want

One aim of our yearly survey is to gauge interest in various new technologies. This year, we asked separately about wireless and management and monitoring technologies. Figure 8, next page, illustrates the results for WLAN technologies that move data, while Figure 9, page 25, illustrates the technologies employed to keep an eye on the system. Though the statistical differences among the survey choices are small, we weren't surprised at the order of responses.

Wireless Technologies

1. High-throughput 802.11n: The term HT (for high throughput) refers to a fully 802.11n network. The 11n specification describes technical methods for reaching theoretical speeds of 600 Mbps—a stunning increase considering that 802.11a/g tops out at 54 Mbps. Actual throughput is always lower due to operational overhead, but 11n introduces vast efficiencies to lower the overhead in comparison to 11a/g. This massive improvement is also accomplished by

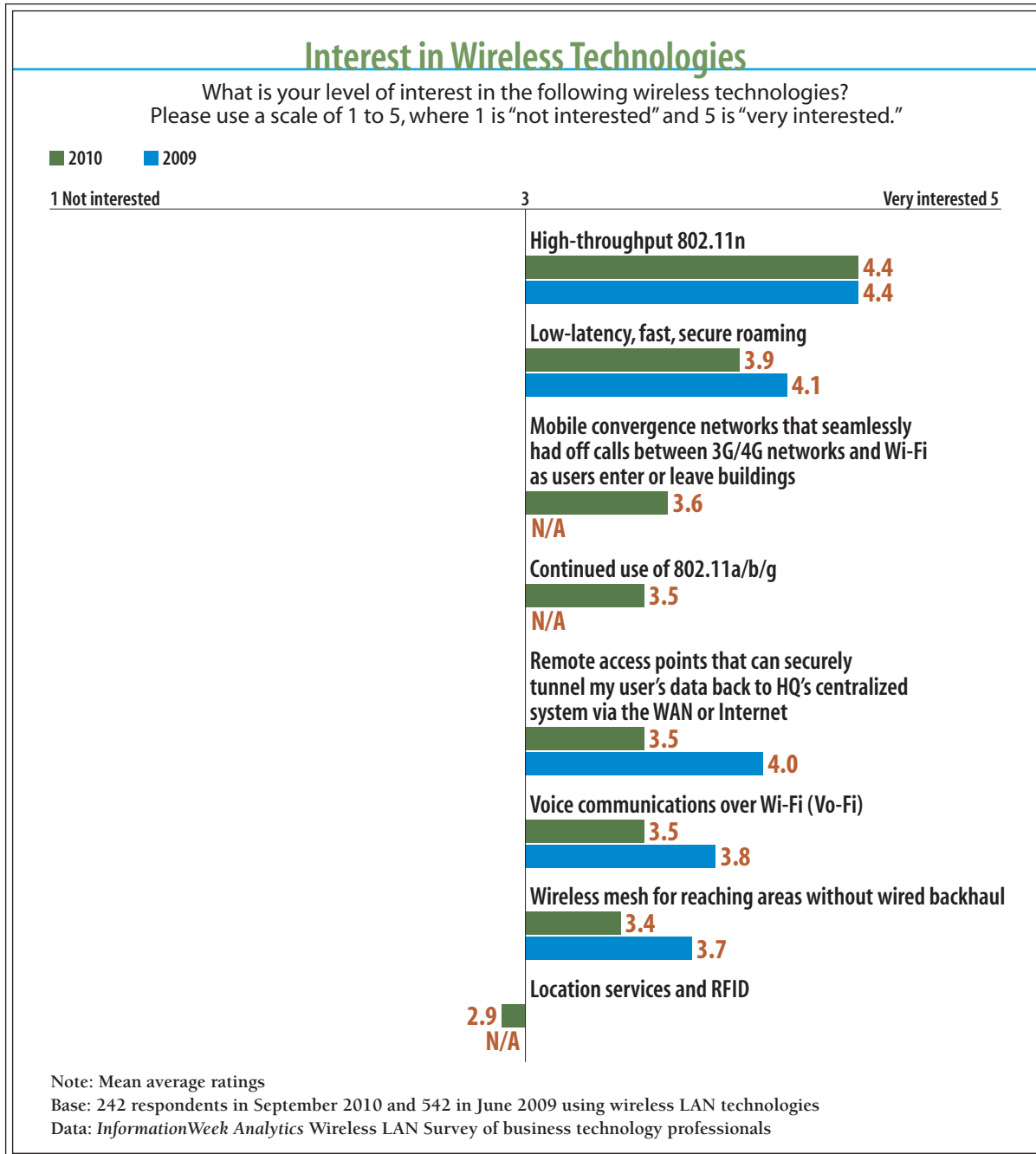
Figure 7





Analytics Report

Figure 8





Analytics Report

a rework to physical-layer communication methods, advanced digital signal processing found in MIMO antenna technologies and improved use of the RF spectrum.

2. Low latency fast, secure roaming: FSR is a WLAN function for maintaining encryption keys as client stations roam. The design goal is to permit clients using advanced authentication and encryption to move from one AP to another and maintain the secure relationship with the network. All of this is done at a speed fast enough to minimize latency, which is important for delay-sensitive applications. The ratified IEEE 802.11r standard addresses roaming, though the function is not yet part of a published Wi-Fi Alliance specification. Currently, de facto vendor approaches are used for FSR. Look for FSR in the Wi-Fi Alliance Voice-Enterprise certification in 2011—we hope—with subsequent inclusion in vendor products.

3. Mobile convergence: The technology might go by various names, but the concept is the convergence of voice and data services within a device. The theory goes, as users with active sessions, such as voice calls, move into and out of buildings, they are elegantly switched between the Wi-Fi and cellular networks without dropping a session. Though there's much interest in it, as Figure 10 indicates, few have deployed it, most likely because the standards-based technology is nascent at best, and vendor-specific technologies are ecosystems of very specific components, making for a harder sell. More on convergence in a bit.

4. (tied) Continued use of 802.11a/b/g: As mentioned earlier, support for legacy access methods are important for a reasonable period of time since it's not practical to replace all devices when an 11n infrastructure is deployed.

4. (tied) Remote access points: Respondents like the idea of APs that, when plugged in at, say, a hotel, securely build IPsec tunnels back to the HQ WLAN. The remote user associates to his portable AP, which then tunnels communications through the intermediate insecure networks all the way to the corporate LAN. Sophisticated authentication mechanisms are a must for this technology so that, if the AP is lost or stolen, an interloper can't access the main network. This is highly useful technology for road warriors.

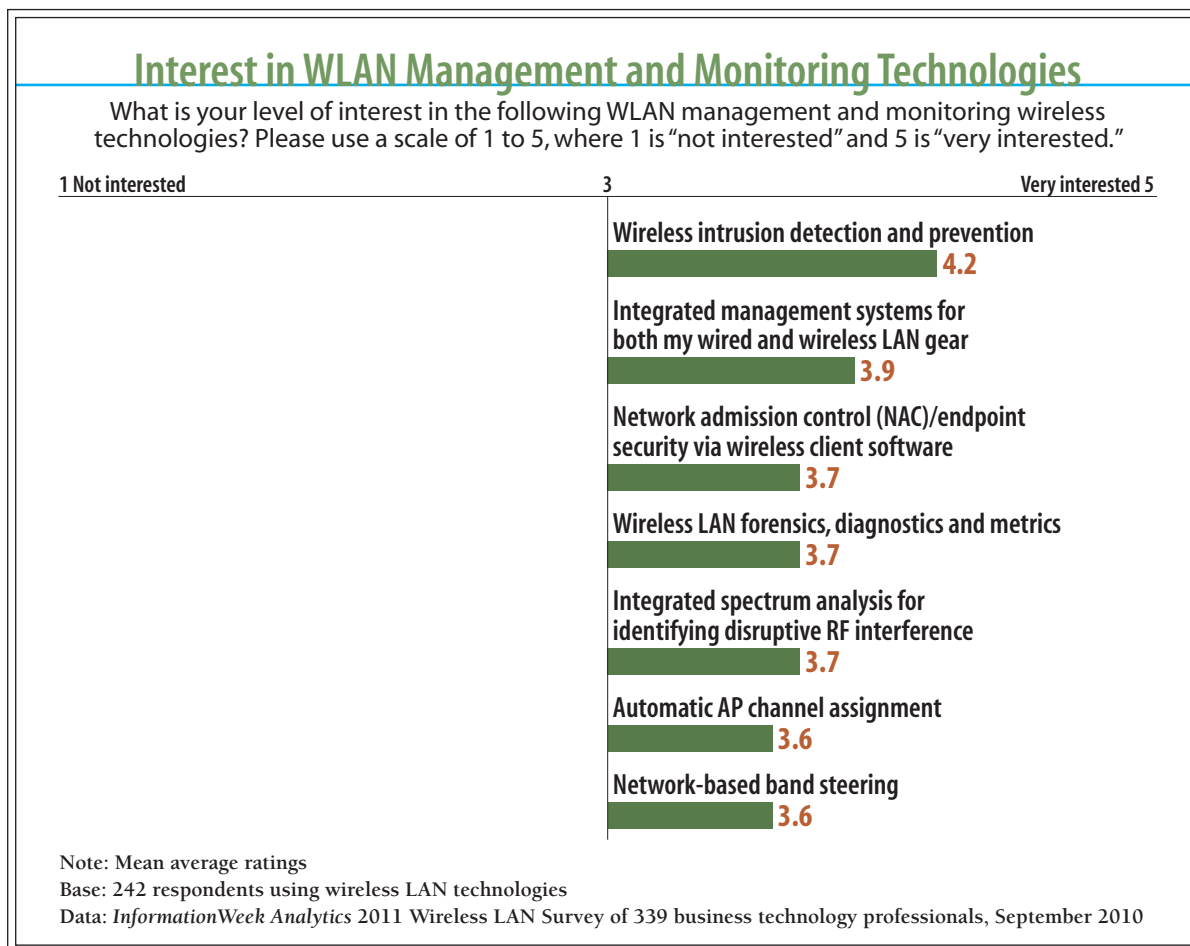
4. (tied) Voice communications over Wi-Fi: We asked a specific question about Vo-Fi, which defines voice calls over a wireless network; as shown in Figure 11, about two-thirds of respondents use it, are testing it or indicate a strong interest. In order to ensure success, these organizations will need to tune in closely to the Wi-Fi Alliance's Voice-Enterprise certification.



Analytics Report

5. Wireless mesh: 802.11s is a draft standard—currently slated for finalization in June 2011—that defines wireless infrastructure device communications using Layer 2 “routing” protocols. More simply put, APs can form wireless associations with one another on one frequency for the purposes of distributing or backhauling data among them and simultaneously servicing client computer associations on another frequency. The end result is that AP units that are completely unwired can coordinate client data transmissions on one radio, while at the same time getting that client data to its ultimate destination on the wired network via the mesh link radio. The underlying mesh protocol determines the best paths to the distribution system using path-costing techniques that take into account such metrics as Layer 2 hop counts and the per-

Figure 9





Analytics Report

formance of various available inter-AP links. Vendors may include these capabilities as part of the base product, while others charge an additional fee to activate mesh functions.

6. Location services: These technologies use access points to measure RF energy emitted from devices you wish to track. Then, using triangulation principles, the item's location is placed onto a map or floorplan so you can go get it.

Management and Monitoring Technologies

1. Wireless intrusion detection and prevention: WIDS/WIPS technology is the watchdog for a WLAN. Full-featured products monitor the RF spectrum and usually classify problems as related to either performance or security. Performance problems, where spectrum is not being used properly, include too many access points on any one channel, excessive retransmissions of data frames or an overabundance of legacy 802.11b clients in the coverage area. Security problems are ones where the WLAN has observed vulnerabilities or deficiencies, such as lack of encryption, or alerts about the presence of a new, previously unknown rogue AP or client. Usually, WIPS technology allows for the triangulation of rogues and mapping of their locations on a scaled floor plan so they can be physically located and removed. Many systems also offer compliance reports to demonstrate, for example, that a WLAN is HIPAA or PCI compliant.

2. Integrated wired and wireless network management: Sure, we all want a one-size-fits-all network management system that addresses the full spectrum of configuration and alerting through a single GUI. But unless you buy all your network components from a single large vendor, you're likely to be disappointed.

3. (tied) Network admission control: NAC technology evaluates the security of end user workstations as they are in the process of connecting to a wired or wireless LAN. NAC is aimed at ensuring devices have the proper patches and antivirus software (among other controls) to prevent the spread of malware. Though NAC is not directly related to the WLAN infrastructure, it can be made part of the authentication process.

3. (tied) Wireless LAN forensics, diagnostics and metrics: These features are far down the interest list—but shouldn't be. Monitoring for interference is key to a reliable WLAN. The most common tools for auditing or problem diagnosis are the ones built into the wireless network management utility you bought with your wireless system, or the ones within an integrated or

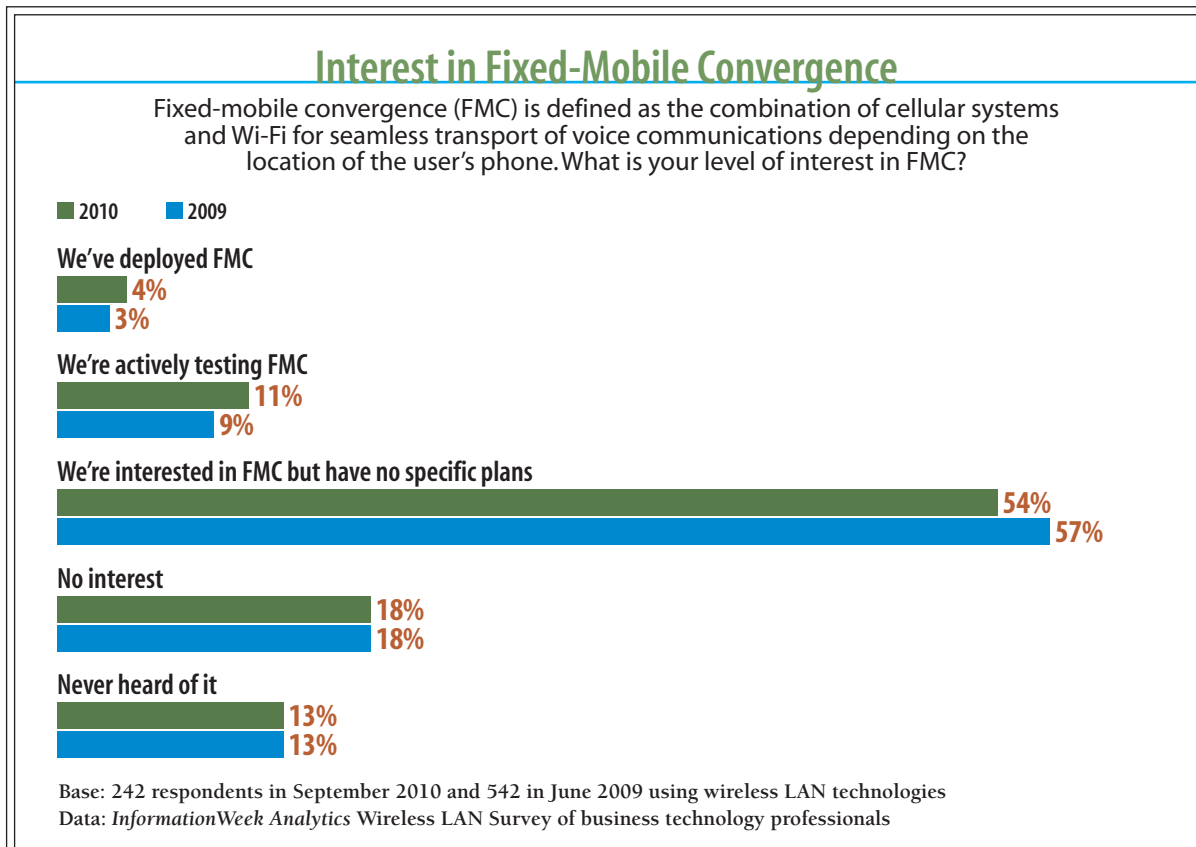


Analytics Report

overlay wireless IPS. Larger enterprise vendors have started building in RF health checks, while other commercial products include spectrum analyzers to evaluate noise and channel usage in the RF spectrum. IT staff also may opt to use wireless packet analyzer tools, such as the popular WildPackets or Fluke's AirMagnet, to provide RF spectrum visibility. More full-featured tools tend to pull data in and perform analysis and interpretation to aid the troubleshooter.

Note that IT staff education is a key component for effective WLAN troubleshooting. We strongly suggest investing the resources and time to understand these often-complex tools. Only when administrators truly understand what the tools are telling them can infrastructure adjustments be made that improve the situation. This results in a better product for end users and ultimately saves the organization money.

Figure 10





Analytics Report

3. (tied) Integrated spectrum analysis: This technology is a reference to tools built into AP units that provide the ability to monitor the RF spectrum for sources of modulated and unmodulated disturbance, such as cordless phones, microwaves and wireless video units. Vendors that integrate this into access points along with a remote management capability—meaning a Wi-Fi expert at the Kansas NOC can look at and diagnose an occasional RF disturbance happening at the Vermont office location—can help drive down operational costs while driving up reliability.

4. (tied) Automatic AP channel assignment: This refers to a system's ability to automatically switch the channels assigned to access points based on environmental conditions. This capability is fairly standard at this point, which may explain its trailing rank.

4. (tied) Network-based band steering technologies: Band steering, or band selecting, is a nonstandard mechanism on the network that helps dual-mode end station devices connect to the WLAN on a preferred frequency. For example, if our preference is to have devices transmitting on the uncluttered 5 GHz band, and a dual-mode device could potentially connect on either 2.4 or 5 GHz, the network will sense the device's split personality and won't answer or talk to it on 2.4 GHz. From the end station's point of view, the WLAN can communicate only on 5 GHz and will thus select that band.

Converged Communications

The worldwide cellular voice and mobile broadband subscriber base is growing at a hyperquick pace, led by a growing array of data-centric devices.

"The current mobile broadband device and phones market is increasingly driven by embedded devices—for example, routers—and smartphones, with injections of growth coming from new touch-screen form factors such as the tablet, notably the Apple iPad, and e-readers like the Amazon Kindle," says Richard Webb, directing analyst for mobile devices at Infonetics Research. "The fierce competition between smartphone operating systems is also pushing the market, with Android and Windows 7 devices showing a strong response to the popularity of the iPhone."

A recent Infonetics report, *2G/3G Mobile, LTE, and WiFi Phones and Subscribers*, shows that smartphone revenue grew to 46% of global mobile phone sales in the second quarter of 2010.



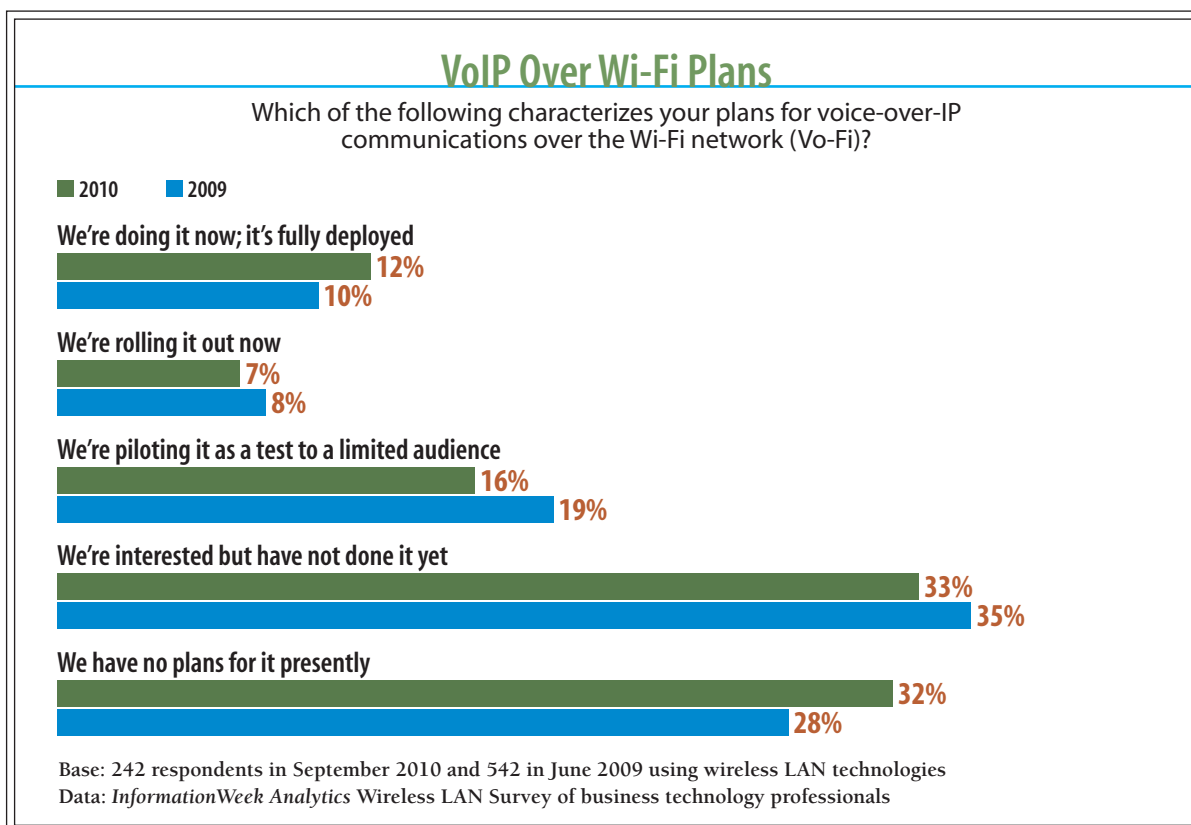
Analytics Report

Infonetics estimates the total current subscriber base at 5.1 billion and foresees an increase to 6.5 billion by 2014, at which time two out of three mobile subscribers in developed countries will utilize a smartphone for network access.

Unfortunately, this smartphone-driven appetite for data is crushing carrier cellular networks. Despite ongoing upgrades from current circuit-switched technologies to data-switched methods like HSPA+ and LTE, bandwidth demand will continue to outstrip supply. Fortunately for carriers, devices these days are often converged, meaning they contain both 3G and Wi-Fi radios. Carriers are exploring ways to offload some data traffic to higher-bandwidth Wi-Fi networks, both to relieve the pressure on their 3G/4G networks and to improve the user experience.

Steven Glapa, senior director of field marketing at Ruckus Wireless, says Ruckus is participating in efforts to define a new “Hotspot 2.0” standard that will address the fundamental chal-

Figure 11





A n a l y t i c s R e p o r t

lenge of taking seamless advantage of Wi-Fi bandwidth—typically a hassle compared with 3G networks, where connectivity and roaming in good coverage areas require no user intervention and are automatic. You simply turn on your 3G device, it finds the network all by itself, and then you communicate. No fuss, no bother. In contrast, Wi-Fi today requires much more manual work of going to a network panel, selecting an SSID and connecting—assuming there is a Wi-Fi network within range to which a user may authenticate.

Carriers and operators want to eliminate this headache. Glapa says that in order to achieve this goal across heterogeneous networks from multiple operators, the same kind of roaming agreements and back-end internetworking systems that developed to support cellular roaming (originally for 2G voice services) will need to be built for combination HSPA/LTE/Wi-Fi networks.

This will happen, but it will take years.

In the meantime, mobile data traffic continues to rise exponentially, and there are operators now implementing Wi-Fi as a 3G data-offload complement. The standards to make subscribers' experiences on their home networks as seamless and effortless on Wi-Fi as they are on 3G exist today and are already implemented on many mainstream smartphones. Achieving this involves leveraging the IEEE 802.1X standard and its EAP-SIM variant for secure, automatic (zero-touch) authentication between smartphones and access points, and the 3GPP 23.234, or I-WLAN, standard to govern how authentication and policy implementation are handled back at the mobile operator's core network.

Glapa says that most operators' current 3G core network infrastructures are capable of supporting enough of the I-WLAN reference architecture to accomplish seamless data offload. Ruckus has demonstrated the ability to implement large-scale networks that use these mechanisms to plug Wi-Fi capacity seamlessly into existing service plans and infrastructures—an absolute requirement for moving quickly, it turns out, because changing the database structure for an operator with 70 million subscribers is a *very* tightly controlled and complicated process, for good reason.

Still, no amount of forward-looking internetworking standards development, or present-day EAP-SIM authentication and back-end network integration, will do anyone any good if smartphone users can't get good high-speed connections over their radio links to the AP. Glapa says that mobile operator network engineering teams always ask one key question up front: "What about interference?"



Analytics Report

This is a hot topic because the high-density urban neighborhoods into which carriers would need to place Wi-Fi to address the most critical smartphone bandwidth shortfalls on their 3G networks are already well populated with access points in the same unlicensed band—usually 2.4 GHz—from collocated enterprise networks and other existing hotspots.

Ruckus' BeamFlex technology uses adaptive smart antenna arrays to reduce interference from the client's perspective, says Glapa, leading to a better connectivity experience in dense urban environments. He also says Ruckus is seeing a fundamental shift in mobile operators' attitudes about Wi-Fi. Rather than considering it a short-term 3G Band-Aid for isolated capacity problems, they're thinking of it more and more as a strategic asset that complements their licensed-band technologies, and will continue to do so in a sustained role over the long term.

This shift is being driven by three basic facts. First, the maturity of Wi-Fi in residential and corporate environments, along with the ubiquity of Wi-Fi interfaces on mobile devices of every type, are driving fundamental changes in subscriber behavior and expectations. When you arrive somewhere and get out your smartphone or iPad, the question isn't "Is there Wi-Fi?" but rather, "How do I log on?"

Second, there is no single network technology that is perfectly suited to every situation. Broad-area coverage and high-mobility users are well served by conventional macro-cellular, licensed-band technologies like W-CDMA/HSPA. Very-high-capacity and -density environments with relatively low subscriber mobility, like classrooms, stadiums or train stations, are well served by Wi-Fi. LTE fits somewhere in between. As skyrocketing bandwidth demand places ever more pressure on all our networks, it makes more and more sense to use the best tool for each network job to optimize performance. Third, demand continues to skyrocket on an exponential curve, while everything operators can do with their networks in the form of more spectrum, LTE and Wi-Fi adds capacity linearly. The network planners we spoke with fully expect to use every technology they can, in combination, just to try and keep up.

802.11n as the Game Changer

Most IT pros are aware of the limitations of 802.11a/g networks. Individual user data throughput maxes out at 22 Mbps even in the most perfect of environments with a single user. In locations with many users, obstacles and reflective surfaces, this number declines precipitously to the point that the network is not usable. Signal reflections cause the condition known as multi-

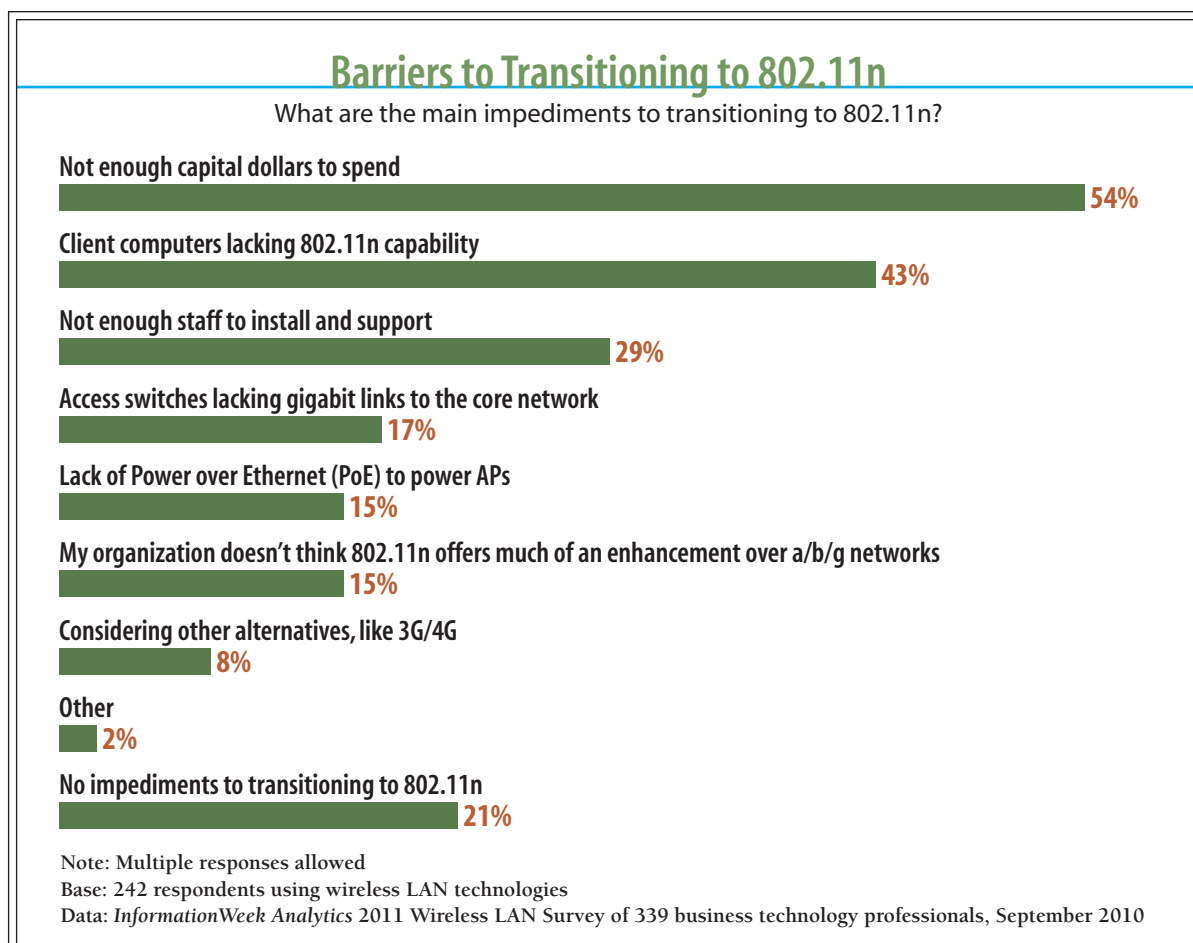


Analytics Report

path, where two copies of the same signal arrive at the receiver at different times, causing loss. This can result in lower data rates and retransmissions.

802.11n technology is a huge leap and is changing the WLAN game altogether. In development at the IEEE since 2004, 802.11n brings a plethora of new technologies that increase data throughput and effective range. The Wi-Fi Alliance states that 802.11n equipment will have five to 10 times the throughput and twice the range of legacy Wi-Fi equipment. Further, it uses radio and antenna technology in clever ways; for example, the multipath that previously made for poor RF environments now suddenly helps. All of this is done with the ability to support legacy devices.

Figure 12





Analytics Report

Though certain sectors, notably retail, healthcare and education, are hot on 802.11n, the main question is, When will enterprises universally jump? As we saw in Figure 4, the coming of 11n itself does not appear to be the catalyst for changing the access layer from copper to RF. This cautious attitude is also revealed in Figure 12. Yes, we continue to weather the worst recession in history. But we (continue to) predict that in time, even the most skeptical among us will be won over thanks to some key 802.11n differentiators. When making the technical case to upgrade, focus on five main areas:

- **Spectrum choice:** 802.11n operates in both the 2.4 GHz and 5 GHz frequency ranges. Access points or end user devices that operate in both—which is really what you want whenever possible—are referred to as “dual-band systems.” The 2.4 GHz spectrum is quite crowded and offers only three nonoverlapping channel choices; you’ll see 802.11n offered here for backward compatibility with legacy devices. But the 5 GHz range is where it’s at: In the United States, there are currently 23 nonoverlapping channels, and it tends to be (for now) smooth sailing. Clean spectrum is good for throughput and reliability. However, note that due to the higher frequency, the laws of physics lower the effective range of these signals compared with 2.4 GHz, meaning you’ll need more access points to cover the same amount of floor space.
- **Channel bonding:** 802.11n allows you to take two neighboring transmission channels and combine them, for the purpose of increasing the data rate. This means that 2x channels is 2x the data rate, all things being equal. Note to techies: Yes, it’s actually slightly more than 2x because there are more sub-carriers with a bonded channel. Also note that channel bonding is advisable only in the 5 GHz range.
- **More efficient transmission:** With 802.11a/b/g, recipients usually acknowledge every data frame that is sent to them. Therefore, you have data/ACK, data/ACK, data/ACK... and so it goes. It works, but it isn’t efficient. In contrast, 802.11n features a variety of frame-aggregation techniques to place several frames of data into one transmission. Acknowledgements can be transmitted in blocks instead of individually. These enhancements increase efficiency and throughput. Buzzwords you’ll see related to this are A-MSDU (aggregate MAC service data unit), A-MPDU (aggregate message protocol data unit) and BlockACK.
- **MIMO signaling:** MIMO, or Multiple Input Multiple Output, is “smart” antenna technology. MIMO units that have external removable antennas tend to have three or six antennas, in

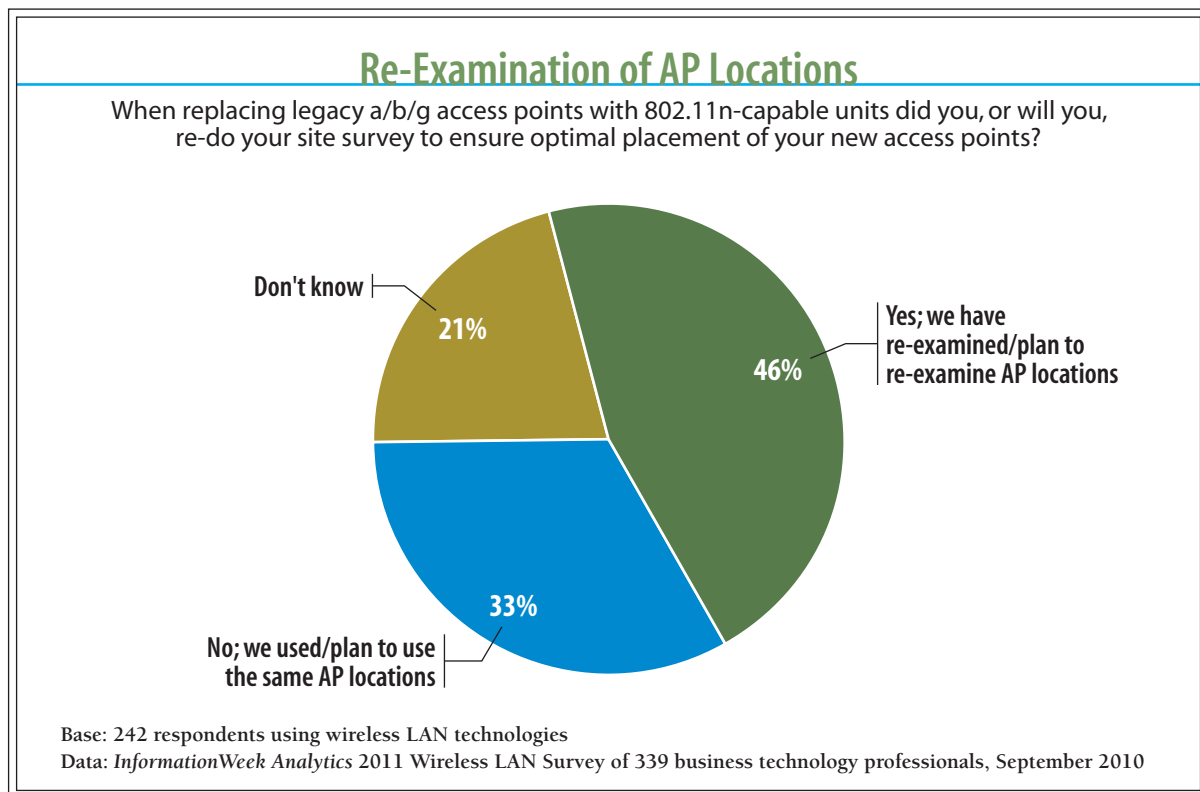


Analytics Report

contrast to legacy units that have fewer. Multipath, where two copies of the same signal arrive at the receiver at different times, may be an enemy to legacy networks, but it's MIMO's friend, since the different signal streams can be used to advantage. In a basic sense, a stream is the same signal traveling down two different pathways due to environmental reflections. MIMO can use these different paths in a variety of ways to increase throughput. MIMO buzzwords you'll see include transmit beamforming, maximal ratio combining, spatial multiplexing and space-time block coding. Bottom line is to watch how the Wi-Fi Alliance treats these techniques from a certification standpoint. Be wary of proprietary signaling techniques that lock you into a particular vendor's products.

- **Legacy tolerance:** 802.11n can play well with legacy gear, though at a cost in performance. Older devices take longer to transmit a given amount of data and to receive the corresponding acknowledgement. While legacy stations are doing their thing, HT stations are waiting

Figure 13





Analytics Report

for their turns to talk. Legacy accommodation should be well understood prior to 11n deployment to determine the operating mode for the WLAN. One strategy is to continue to use the three usable channels in the 2.4 GHz spectrum for older client devices and reserve the 23 usable channels in the 5 GHz spectrum for your 802.11n deployment. This enables both to operate as efficiently as possible without affecting the other.

Other new technologies included with 802.11n are power saving modes for client devices and the ability to tweak what's known as "guard interval" settings. By reducing the time between transmitted signals, more throughput can be realized. The downside for highly reflective environments is that retransmissions can reduce throughput, so modify this setting with prudence.

When architecting an 11n network, we *highly* recommend that you plan to the lowest common denominator—defined as 5 GHz UNII spectrum with -65dBm or better signal strength throughout. By doing so, the network should be able to support excellent data rates and seamless roaming, even for demanding Vo-Fi applications. Keep in mind that the laws of physics mandate that, due to their longer wavelength, 2.4 GHz signals propagate further than 5 GHz signals at the same AP power levels. To have both spectrums cover roughly the same amount of area, the rule of thumb is to plan for 2.4 GHz radios at about half the power output compared with 5 GHz radios. If you're converting an existing WLAN to a dual-band 11n network, the current AP locations are often not entirely suitable. Therefore, it's important to conduct a new site survey based on updated specifications. As Figure 13 indicates, almost half of respondents know this is a good idea.

If you already operate a dual-band 11a/b/g network, the good news is that fewer dual-band 11n access points are normally required for the same signal strength coverage because of 11n's better digital signal processing capabilities. These assumptions can be quickly verified using predictive site survey tools, such as those from Ekahau.

No Free Lunch

All this sounds great, but we're sure that by now you're thinking there must be a catch. Well, we contend that the upsides of 11n are huge and that you must simply plan to handle the requisite new-technology bumps that always occur during significant transitions. Still, we do have some gotchas that those considering an upgrade need to watch for.



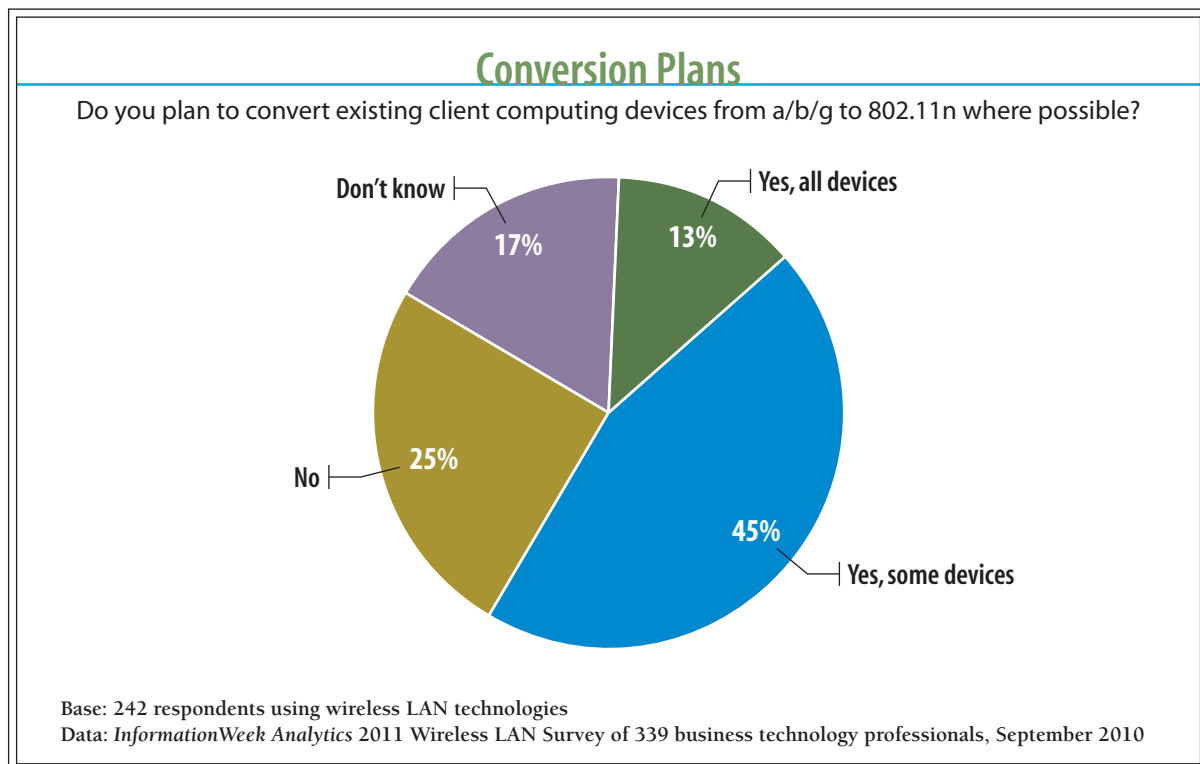
Analytics Report

First, we've been focusing on the back-end infrastructure of the WLAN. But remember that client stations must be 11n capable to take advantage of the new technology. If all of your end user devices are 11g and/or 11a, then you've got to either replace them or swap in new wireless NICs and the drivers and software supplicants that control the cards.

"The client side is a huge challenge to infrastructure vendors, and the varying quality of client device chipsets and drivers is wreaking havoc with overall network reliability and consistency," says Devin Akin, chief Wi-Fi architect at Aerohive. Based on our own experience, we couldn't agree more. Ask your WLAN infrastructure vendor if it has conducted tests and thus can recommend hardware and driver combinations that have proven to work well together. As Figure 14 indicates, more than half of those surveyed plan to retrofit some or all end user devices, whereas 25% have no plans to convert existing devices at this time.

As your plans solidify for the back-end portion of the rollout, take time to succinctly define the

Figure 14

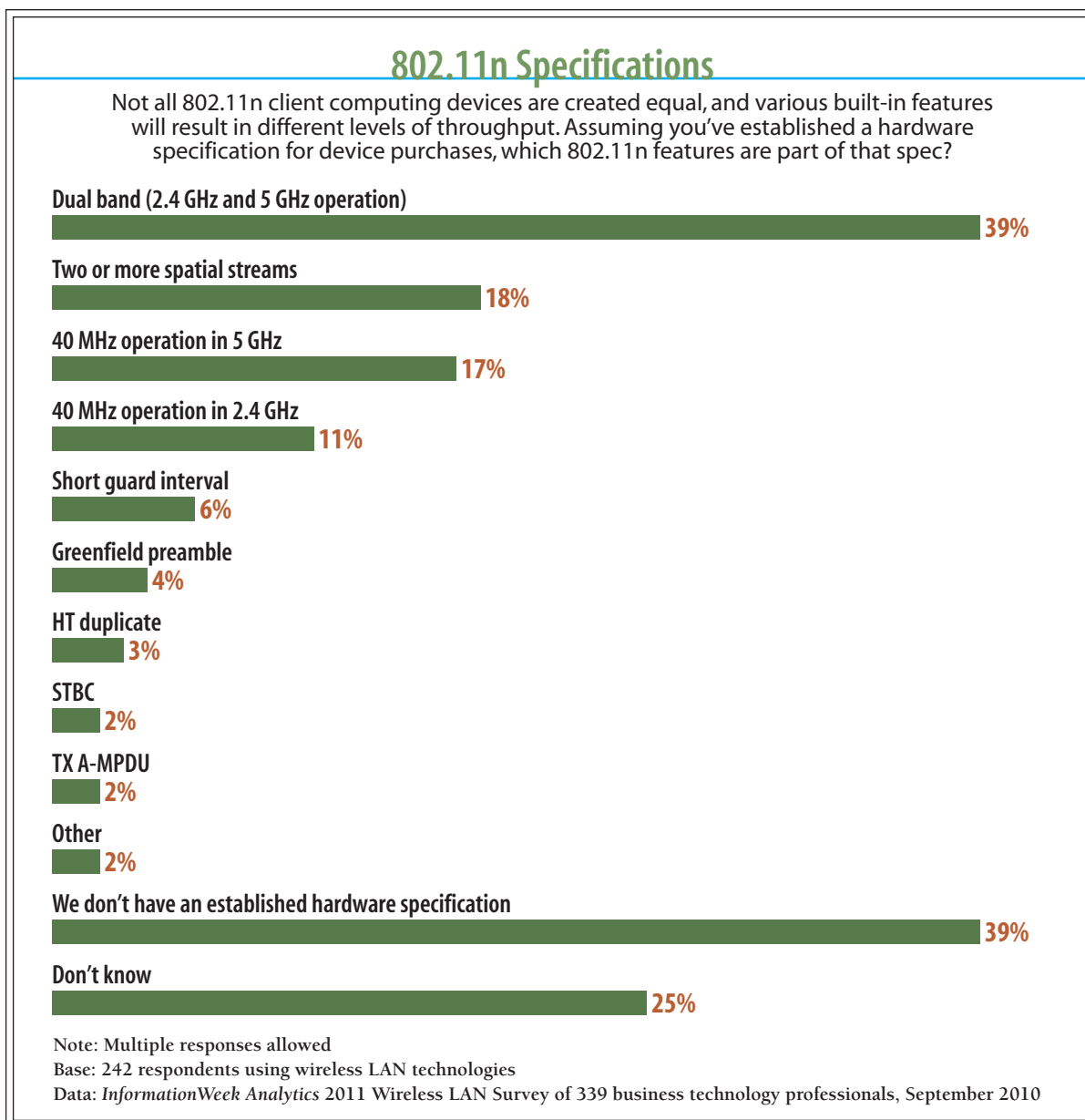




Analytics Report

features and functions for the client side in a specification used during purchases. Most importantly, we recommend the purchase of dual-band NICs that operate in the both the 2.4 and 5 GHz spectrums. It is beyond us why vendors are selling laptops without the ability to

Figure 15



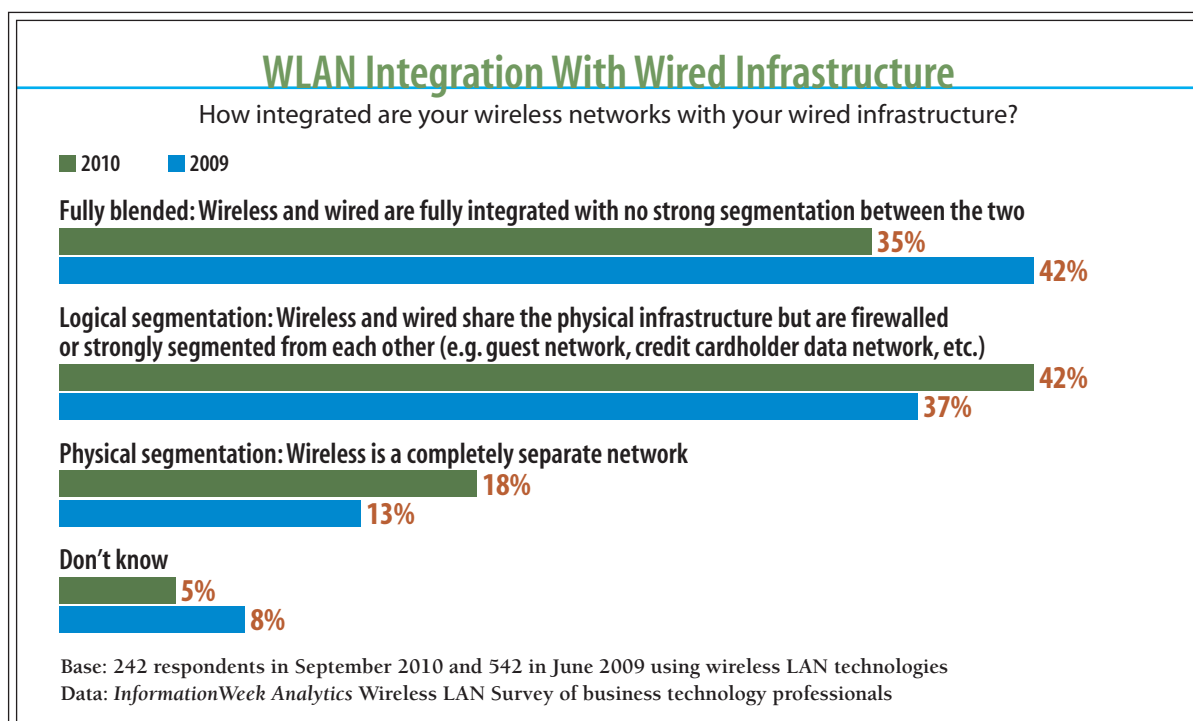


Analytics Report

use 5 GHz, because even though they may be 11n capable, the 2.4 GHz space is so noise polluted in most places, one never realizes 11n's promise. In addition, pay particular attention to a Wi-Fi card's support for spatial streams—currently 1, 2 or 3—as well as its ability to utilize 40 MHz channels, as both of these directly drive throughput potential. If you're not sure what a device can do, visit the Wi-Fi Alliance Web site to look up the specifications of the product in question.

Moving away from client-side issues, 802.11n APs have more circuitry and radios installed and often need increased power to drive them to full capability. Even if you have standards-based 802.3af Power over Ethernet (PoE) switches powering your legacy AP units, the 15.4 watts provided by this type of PoE will not always fully power 802.11n circuitry. You may need 802.3at PoE, which was ratified by the IEEE on the same day as 11n and is built into switches or external power-injector devices. If vendors claim that their 11n access points are able to function on legacy 802.3af power, get proof that this is so before signing a P.O.

Figure 16





Analytics Report

Finally, there's your wired network to consider. 802.11n devices are able to send and receive far more data than legacy devices. These new APs will have one or more Gigabit Ethernet ports versus the typical 100 Mbps ports on legacy gear. If you're planning to run at the new higher speeds, consider Gigabit links to each AP.

Of course, networks can be architected in many ways, and AP-to-switch Gigabit links are not necessarily required as long as you realize that the client-to-AP throughput will max out at the speed of the AP's wired side. For example, even though the AP may be able to service 300 Mbps aggregate on its wireless side, if it is wired into a 100 Mbps switch port, wireless users won't see any more than 100 Mbps to destinations on the wired network.

On a related note, backhaul links from the access switches in your wiring closets down to distribution or core switches may need to be upgraded to multi-gigabit links, especially if the access switches have many high-throughput APs attached.

We'll address Wi-Fi architecture bottlenecks and situations where too many HT AP units are pushing data to too few controllers in the next section.

Architectural Matters

When wireless first started to make its way into the enterprise, it was often deployed as a completely separate network. This was done for a handful of reasons, often security concerns with WEP. Or, maybe the infrastructure staff wasn't ready to deploy wireless, but another group forced its adoption for one reason or another. The compromise was usually to keep the networks isolated.

Today, the typical setup—regardless of industry—is wired and wireless access methods living alongside one another on separate broadcast networks but meeting at some point within the infrastructure. The degree to which the WLAN is integrated into the wired network does vary, but the trend is definitely toward complete integration since operating two infrastructures is far too costly. Figure 16 shows that a sizable majority of our survey respondents either fully blend their networks or use logical segmentation of some sort.

Integration fears are assuaged with the proper use of wireless security, though as we'll see later, this component of the technology is still not well understood. Other controls outside of the

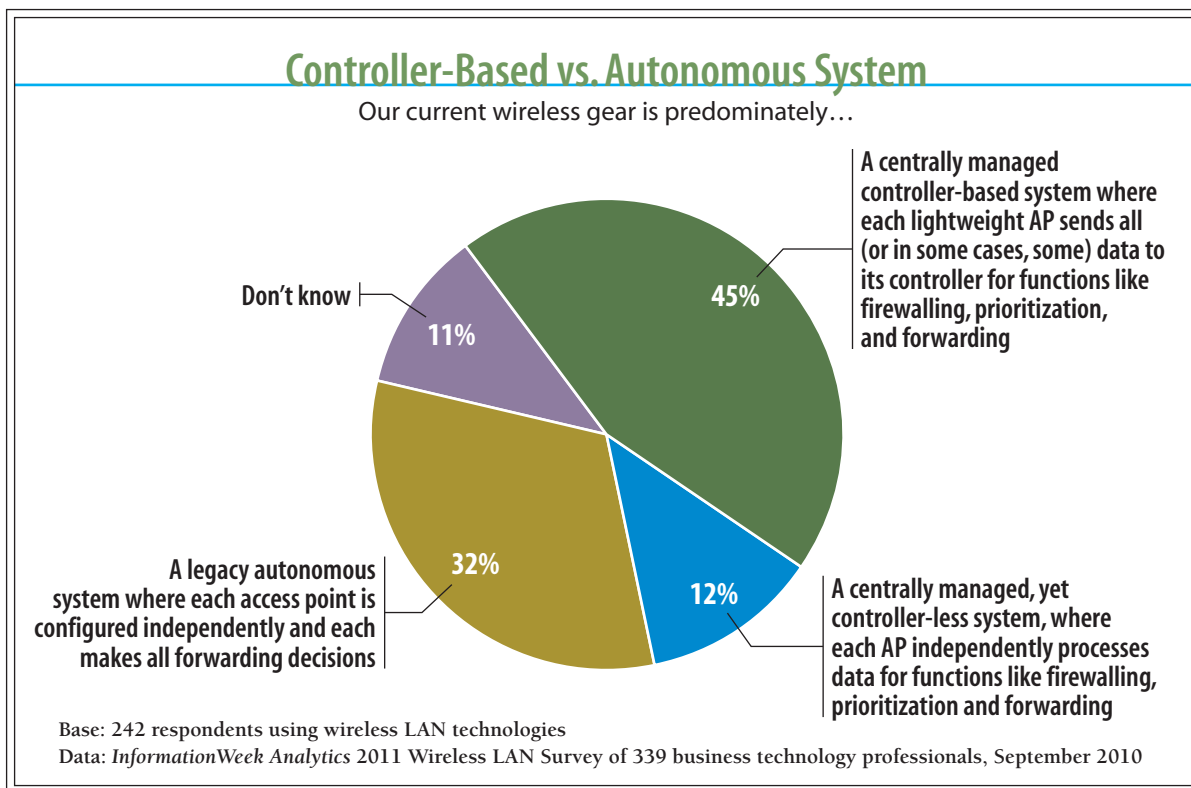


Analytics Report

802.11 standard, such as firewalling and role-based access control, are also often implemented for the purpose of determining which users can interact with which systems in what ways and at what times of day.

When 802.11 first arrived, WLANs were made up of fully distributed autonomous access points. Each AP was configured independently and was tasked with sending data to a wired distribution system, from which traffic made its way to the destination. Autonomous APs, especially from the biggest vendors, didn't generally form relationships with one another and were ignorant of neighboring APs. These autonomous networks required significant manual tuning and guesswork to achieve the most effective settings. This approach eventually evolved into a more centralized model, where there is a central "brain" that controls most operational aspects. AP units form relationships with the controller and then shuttle frames to and from the RF environment and the Ethernet backhaul. Access points are often "aware" of their neighbors for

Figure 17





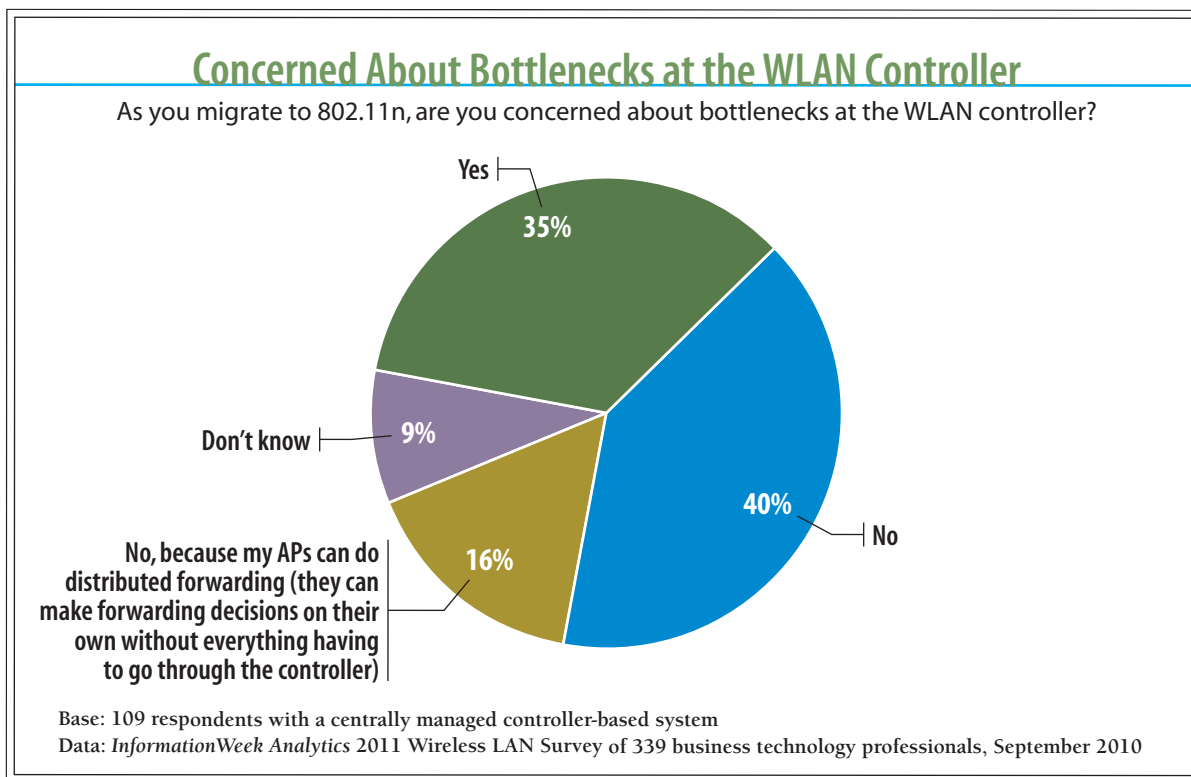
Analytics Report

purposes of power management and client roaming. Today, most enterprise vendors take a centralized controller focus.

But now, another upheaval is at hand. Vendors have recognized that in light of 11n's ability to jam much more data between the RF and copper, there are scaling limitations around sending this data volume at a controller for a "what's next" decision. "The rapid adoption of wireless applications in the workplace is putting much greater demands on today's wireless LANs," says Alan Lopez, wireless LAN solutions manager for Motorola Solutions. "For the best user experience, network capacity has to increase while maintaining resilience and security and avoiding bottlenecks at the wireless controllers."

Lopez is referring to the *new* distributed model, where access points have relationships with a controller but don't rely on it for forwarding and policy decisions, such as quality of service and firewalling. We pointed out a year ago that Aerohive has been a leader of the "no con-

Figure 18





Analytics Report

troller” mantra (its Hive Manager appliance is more of a configuration platform operating on the management plane). This is still the case, and curiously, some big vendors, including Aruba and Motorola, have been converting their platforms to follow suit. Cisco, however, appears to not be evolving its architecture in this way, likely because doing so would cannibalize its current business. We think that the new distributed model is the way to go, but caveat emptor. Make sure that any candidate vendor is indeed processing *all* data-plane (forwarding operations) and *all* control-plane (policy operations) at the AP and not the controller. Some vendors are able to do this only partially or have limits on the number of access points that can operate fully distributed. Figure 17 shows the mix of WLAN architectures in use by our respondents.

As shown in Figure 18, the 109 respondents using central controllers weighed in on whether they were concerned about bottlenecks within their infrastructures. The results show that 44% are either worried or unsure of their situation, which equals opportunities for vendors offering this technology.

WLAN Vendors

We asked poll respondents, “Which wireless vendors do you use?” Multiple responses were permitted. Like last year, the market share rankings in this survey are not scientific, but answers ran the gamut of pretty much every manufacturer of WLAN gear, from SOHO-class autonomous APs to controller-based lightweight systems to modern distributed-architecture intelligent APs to single-channel architecture systems. It’s no surprise that Cisco commands the most market share. We are amazed, though, that such a large percentage of respondents still use older autonomous access point gear.

When will these die?

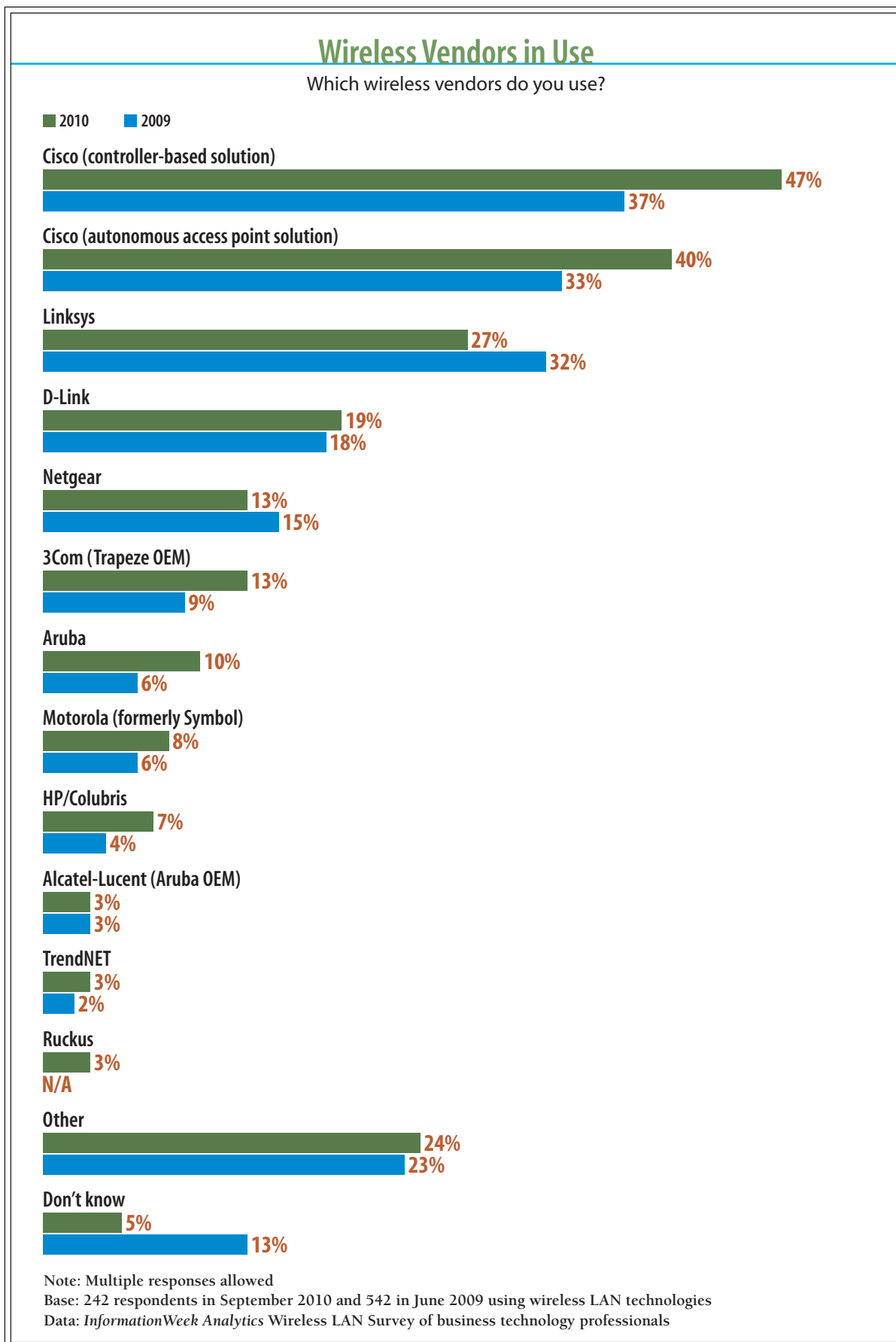
While on the subject of vendors, we also wanted to find out the most important factors when IT is evaluating candidates. Not surprisingly, the top areas respondents look for are reliability, security, performance and scalability, all unchanged from 2009. These results are consistent with Figure 1, where we rank performance, reliability, security and consistency as the top four reservations respondents have about wireless LANs as the predominant connectivity medium.

Reliability is No. 1 all around. For all but the most casual-use WLANs, Wi-Fi infrastructure for business must have wire-like reliability to support demanding applications and to satisfy the



Analytics Report

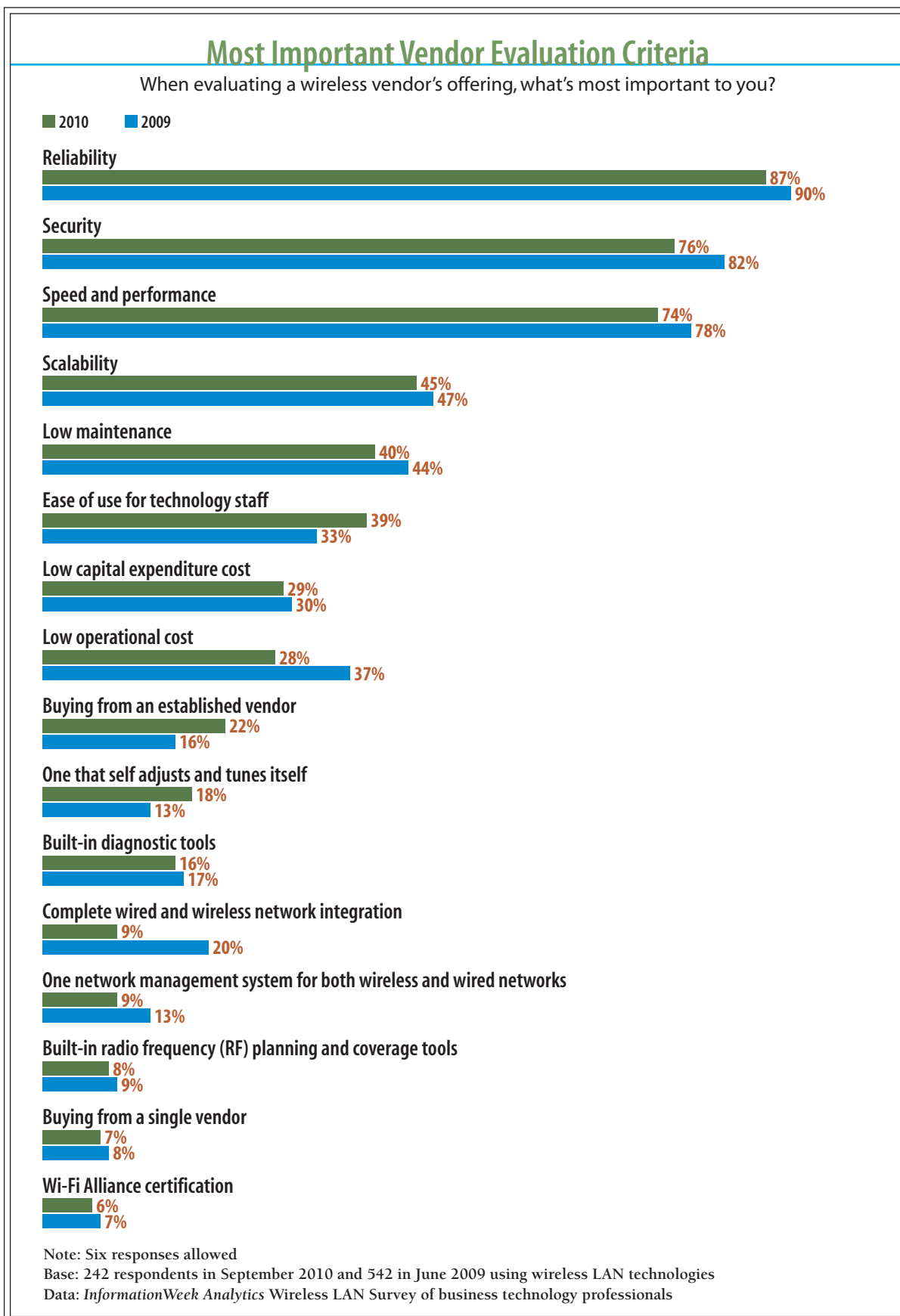
Figure 19





Analytics Report

Figure 20

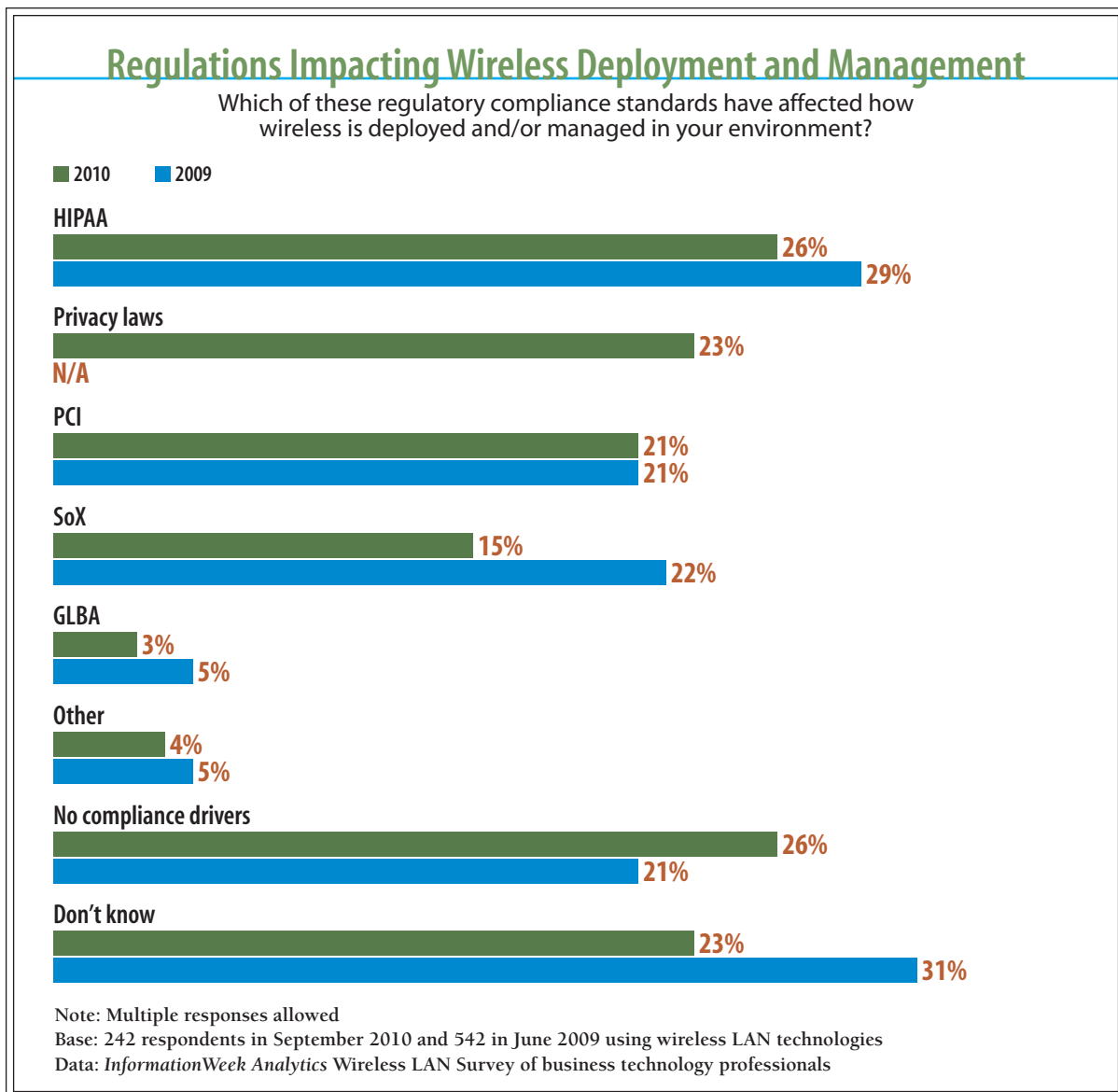




Analytics Report

always-on requirements of users wherever they happen to be. As such, CIOs must not be afraid to take wireless vendors to task and insist that they demonstrate best practices for a successful deployment in the actual environment. Ask for a proposal that maximizes the qualities most important to you. But in turn, CIOs must be prepared to make the needed investments in WLAN planning, vendor tools that make it easy to track the network's health, and staff

Figure 21





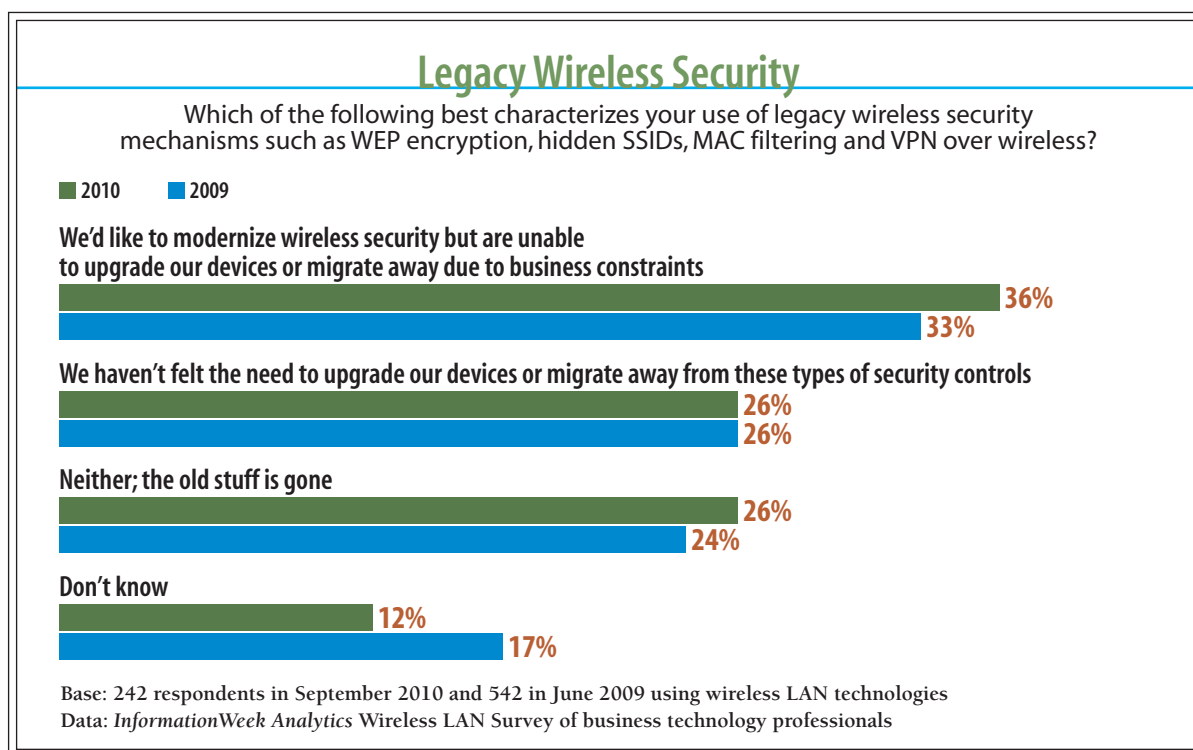
Analytics Report

resources and training. Mission-critical Wi-Fi is a new animal to most IT pros, 11n is a big change from previous iterations of the spec and achieving adequate security requires some specialized know-how.

Regulatory Compliance and WLAN Security

A significant concern for information security teams is that sensitive information could be vulnerable if it traverses a wireless network, or if somehow a WLAN is “connected” to systems containing this data. Companies that need to comply with regulatory requirements must also take rules governing WLANs into account. For example, the Payment Card Industry’s Data Security Standard (PCI DSS) specifically states that “if wireless technology is used to store, process, or transmit cardholder data, or if a wireless local area network (WLAN) is connected to, or part of, the cardholder data environment, the PCI DSS requirements and testing procedures for wireless environments apply and must be performed.” In a nutshell, PCI DSS requires

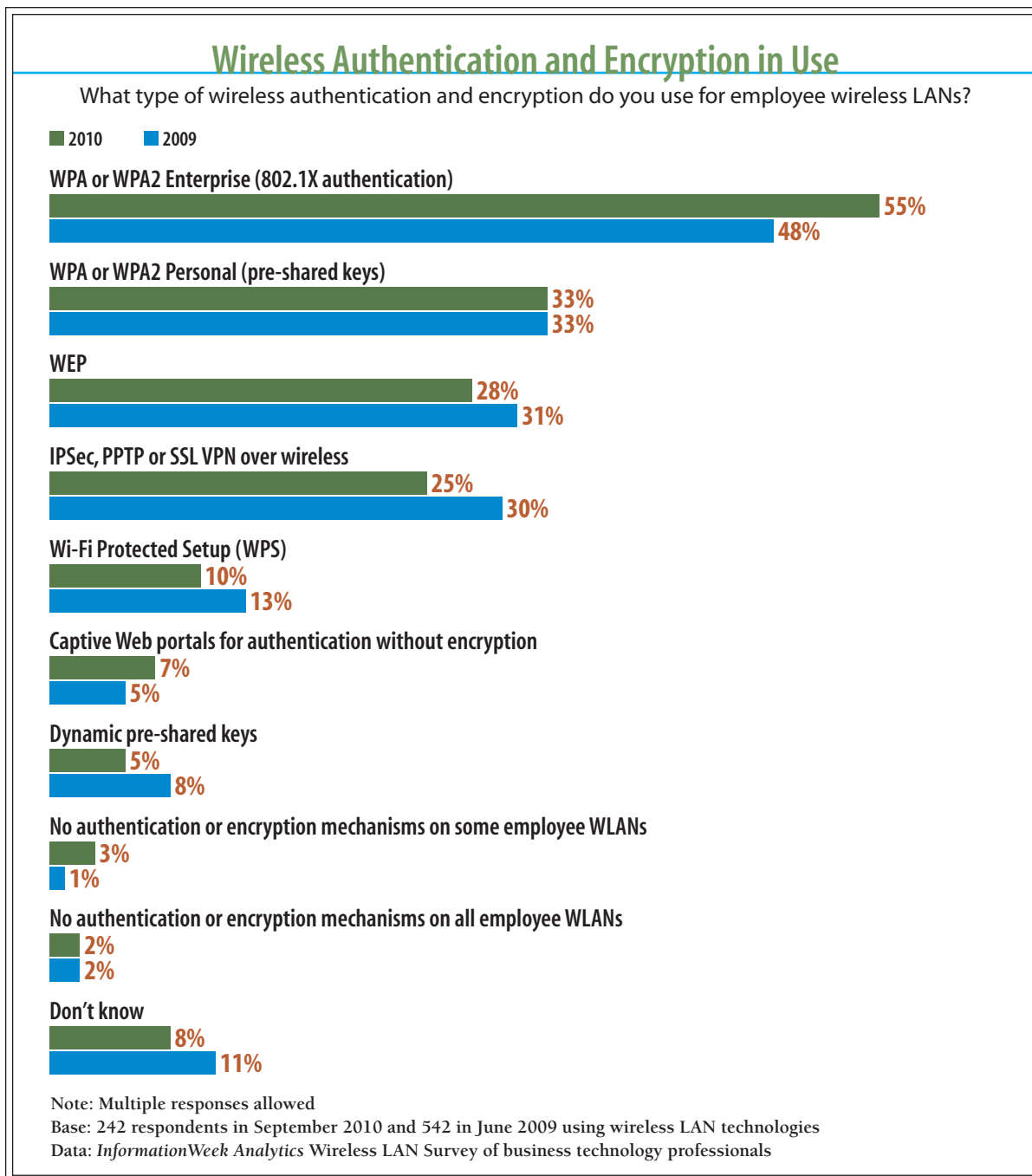
Figure 22





Analytics Report

Figure 23





Analytics Report

the use of firewalls to segregate Wi-Fi networks from networks that contain cardholder data, use of strong encryption and periodic scanning for rogue access points. HIPAA, another ubiquitous compliance hurdle dealing with protections of personal health information, is not as specific as the PCI DSS, but it is clear that using open or weakly encrypted/authenticated networks would result in a black mark.

Furthermore, states are beginning to adopt ever-more-stringent privacy laws that directly affect businesses, with steep penalties for those not able to demonstrate due diligence.

We understand the concern—an unsecured WLAN certainly poses a greater risk of unauthorized access compared with a wired network, given the accessibility of the physical medium. Figure 21 illustrates some of the top compliance regulations and standards that affect our respondents' infrastructures. Companies subject to these regulations must enforce privacy, transmission integrity and strong authentication within their WLANs. How?

- Use **strong encryption**, preferably CCMP/AES (WPA2);
- Use **strong authentication**, preferably multifactor methods that leverage 802.1X/EAP (WPA2-Enterprise);
- Ensure a documented **wireless use policy** is available and enforced;
- Integrate smart **operational procedures** into the environment to monitor, manage, update and secure all WLAN devices and user systems; and
- **Segment and monitor** the WLAN. In some cases, as with PCI, WLANs must be firewalled off from the environment that contains sensitive data.

There may also be controls specific to individual regs. In our experience, however, once IT groups understand the nature of Wi-Fi technology, it becomes apparent that it is no more difficult to protect these devices, just a bit different.

We were curious about the evolution of legacy security use in the enterprise since our previous survey. WEP, SSID hiding and MAC filtering can all be cracked within minutes using easily acquired open source tools. Though widely publicized as ineffective, as Figure 22 indicates,



Analytics Report

these mechanisms are still in use by 26% of our survey respondents. This simply amazes us and borders on reckless. As the regulatory environment becomes increasingly focused on maintaining privacy and proof of information-protection due diligence, C-level management in these organizations should ask themselves, “Do we look good in orange jumpsuits?”

VPN over wireless, though capable of providing data privacy and user authentication, cripples WLAN performance because users who roam while having the VPN connection up must generally recreate their VPN connections every time.

Those who’ve ejected legacy mechanisms should be congratulated. Further, as the numbers in Figure 23 indicate, there has been an uptick in enterprise-grade security that uses extended authentication. This is good.

So what should everyone be doing? When at all possible, opt for WPA2-Enterprise using one of the seven 802.1X/EAP variants for client and network authentication. The EAP method you choose is driven by the back-end directory, most often Microsoft Active Directory, where user accounts or digital certificates are stored. Note that WPA2 is *required* for use with 802.11n in order to realize 11n speeds. Otherwise, your 11n throughput will resemble 11a/b/g networks and you’ll be left scratching your head.

For smaller implementations, Wi-Fi Protected Setup (WPS) is a decent choice for provisioning devices without having to reveal the secret passphrase upon which encryption relies. Though WPA/WPA2 Personal is acceptable for small environments, be wary of any sort of preshared-key security, not because it can’t be made secure, but because, depending on the quantity of devices you manage, it may be unwieldy. For example, each device in a preshared-key environment must have the key entered individually. If any device that uses a key is lost or stolen, the key is considered compromised—as is your overall security posture. To rectify the situation, each remaining device must be manually reconfigured with a new preshared key.

Dynamic PSK is also a configuration method for preshared key environments, but potentially more scalable within the SMB market. Captive portals offer “Web” authentication similar to what’s used in hotels and is usually used for guests, while IPSec VPN over wireless is legacy technology—it can be secure, but it limits a WLAN’s flexibility.

As for WEP, don’t use it. Period.

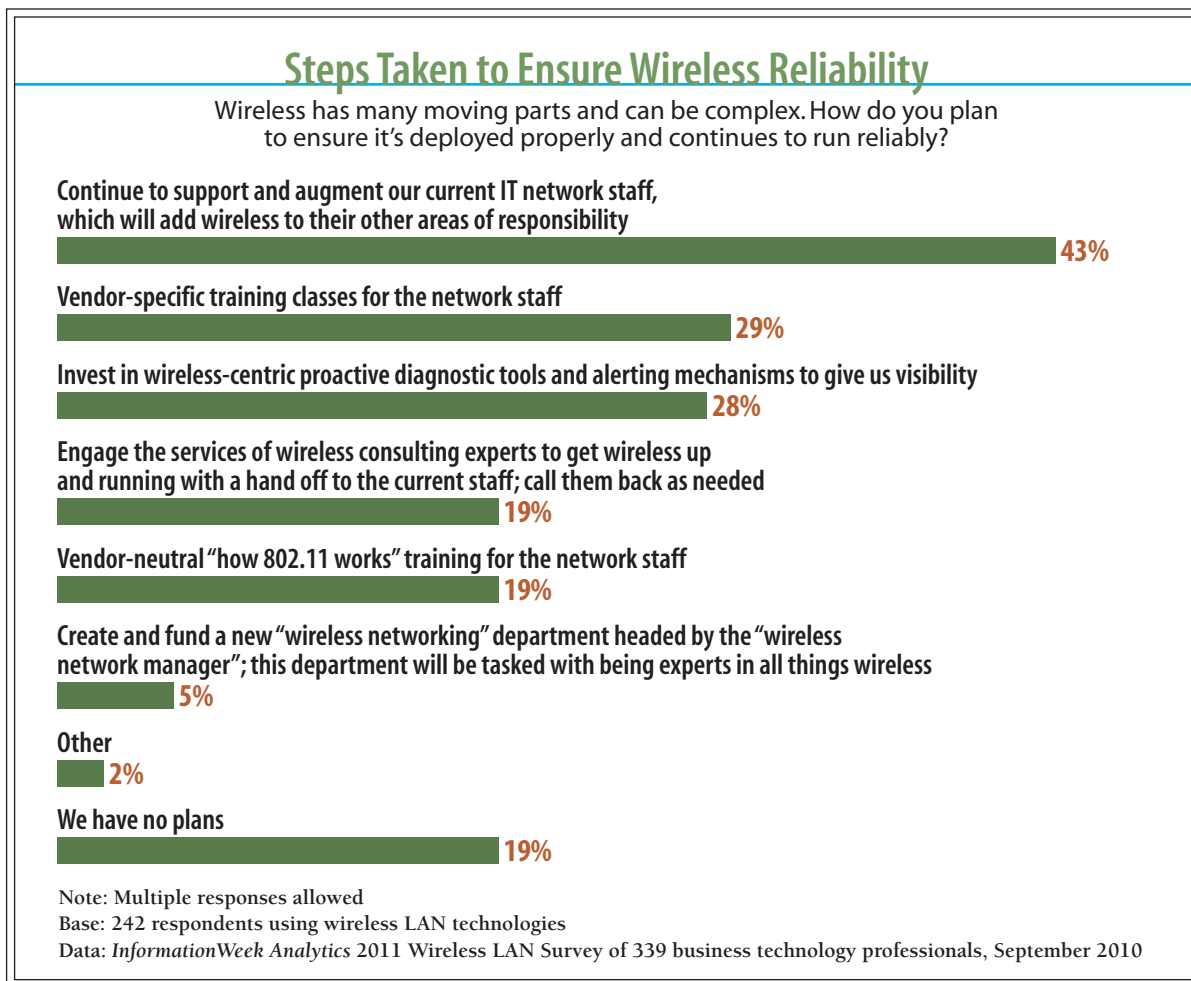


Analytics Report

Education's Role

Though wireless has been around for a decade, our experience indicates that it is generally poorly understood. Technologists responsible for WLANs get a sense of what works and what doesn't in their environments. They also get to know the product GUIs after time spent using them. But what we see out there is a general inability to explain what is happening under the wireless hood and to really use diagnostic tools to any mid- to advanced-level degree. Because of this, institutional knowledge tends to be quite ad hoc and observational in nature. This needs to change.

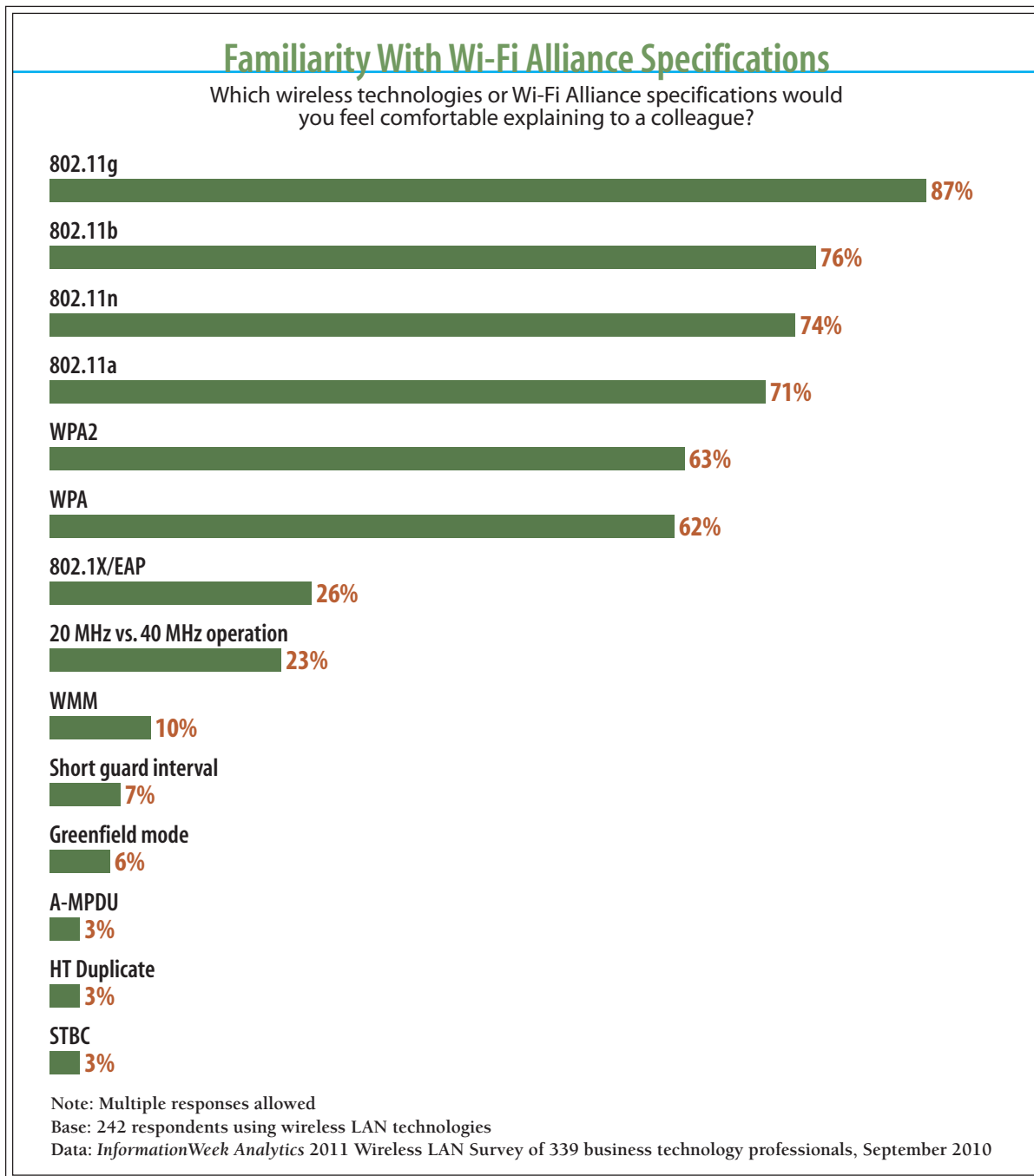
Figure 24





Analytics Report

Figure 25





Analytics Report

With 802.11n, wireless is poised for much deeper penetration at the access layer since speeds will be comparable with 100 Mbps Ethernet. Therefore, wireless reliability is important. As Figure 24 indicates, it doesn't look like any special "wireless departments" will be created, and wireless specialty consultants will be used only some of the time. Current staff will take on the bulk of the responsibility for keeping 11n WLANs up and secure. Many will have a difficult time learning the facets of this new and very complex technology, especially in shops where economic conditions have forced cuts and staff is stretched to keep the lights on. Bottom line, CIOs need to invest in training if they expect to reap the full benefits of their wireless investments.

As we discussed last year, a multistep approach to wireless education delivers the best value.

- **Expose staff to the guts of wireless technology.** We're not talking about vendor-centric training; instead, start with vendor-neutral wireless courses like those offered at CWNPN.com. The Certified Wireless Network Professional education and certification initiatives, some of which we teach, bring network administrators and consultants up to speed on 802.11 technology without drowning them in vendor speak. As Figure 25 illustrates, there are many new terms and technologies to be learned.
- **Understand the WLAN organizational requirements** handed down from management. For example, are WLANs for casual guest networks? Or are they considered mission critical? What are the desired coverage areas? What are the security and performance requirements?
- **Read and understand your chosen vendors' specific design guides.** Call your sales rep and get a system engineer on site to whiteboard ideas and approaches. Already have a WLAN in place? Request a free design review, which most vendors will do in hopes of selling more gear and software. These whiteboard sessions are a great avenue for learning about GUI buttons and knobs previously unseen, unused or misunderstood.
- **Now it's time for formal vendor training.** Get your staff out of the office for a multi-day training event that is specific to the vendor gear you've chosen. By this time, they'll know how wireless works and the organization's WLAN mission, and now they'll have a chance to test drive specific GUIs and gear and learn how your vendor implements standards-based technology.



A n a l y t i c s R e p o r t

- **Budget for lab gear and diagnostic tools** such as spectrum analyzers and wireless frame analysis software. If you're using a controller approach, most vendors have low-end controllers that can be had for \$2,000 to \$3,000 and added on to a few access points. If using distributed AP gear, buy extras for the lab. Consider spinning up a virtualized back-end authentication system for testing to make the lab fully functional.

Education is paramount to the success of any large-scale WLAN initiative; if your organization is considering deploying to more than 100 people, the education component is but a small portion of the capital expenditure of the entire system. The Certified Wireless Network Professional alliance (www.cwnp.com) offers multiple levels of vendor-neutral, enterprise wireless LAN certifications, from novice to expert:

- **CWTS:** The entry-level Certified Wireless Technology Specialist certification validates the knowledge of enterprise WLAN sales and support professionals who must be familiar with the terminology and basic functionality of enterprise 802.11 wireless networks.
- **CWNA:** The Certified Wireless Network Associate certification, the most popular variety, validates a networking professional's wireless knowledge foundation. CWNA covers topics such as basic RF theory, 802.11 implementation types, wireless frame exchange processes, WLAN analysis, the basics of security and more.
- **CWSP:** The Certified Wireless Security Professional certification is all about WLAN security and advanced design concepts.
- **CWDP:** The Certified Wireless Design Professional certification prepares WLAN professionals to design wireless LANs for different applications and to ensure they'll perform optimally in varied environments.
- **CWAP:** The Certified Wireless Analysis Professional certification prepares WLAN professionals to analyze, troubleshoot and optimize any wireless LAN.
- **CWNE:** The Certified Wireless Network Expert certification assures that candidates have mastered all relevant skills to administer, install, configure, troubleshoot and design wireless network systems. Protocol analysis, intrusion detection and prevention, performance and QoS analysis, spectrum analysis and management, and advanced design are some of the areas of expertise that are required.



A n a l y t i c s R e p o r t

Conclusion

We've covered a lot of ground in this report, from 11n to architecture to education. To sum up the key takeaways, first understand that a number of *InformationWeek Analytics* surveys—and our experience—confirm that organizational mobile and portable device purchases are increasing rapidly. Further, according to the Wi-Fi Alliance, there will be a doubling of Wi-Fi devices worldwide this year alone. Solid wireless network infrastructures are needed to effectively support them.

A large percentage of respondents are currently using wireless LANs, and 58% see their 11a/b/g networks being retired within three years. These facts point to WLANs supplanting wired access networks in many shops. Of course, as with any technology advance, upgrades will be incremental, but where 11a/b/g networks are overwhelmed by new end user devices, expect tech refreshes to come quicker—especially when WLAN vendors can point with more certainty to improved ROI, and new applications that benefit from mobility are launched.

When researching WLAN purchases, have vendors articulate how capex and opex costs will compare with copper. Vendors also need to make a good case for how their technology preserves critically important reliability and consistency. Ask what technologies or infrastructure modifications outside of the vendor's offering should be evaluated to augment your goals. Make it a point to understand the vendor's recommended network design guides. This will uncover other changes that may be needed in your infrastructure and that may affect the overall budget.

Even if money is still tight, begin planning for 802.11n high-throughput WLAN gear. Consider how you can simultaneously support legacy and new device types, apportion RF spectrum, and architect the WLAN network itself.

Be aware of 802.11n prerequisites. Since 11n networks can be much faster than legacy 11a/b/g, data bottlenecks are more apt to occur on the wired infrastructure side. Controllers can be bottlenecks, too, so consider fully distributed architectures—ones that don't rely on controllers for firewalling, data prioritization or data forwarding—but that are still centrally managed.

Realize that 11n access points, depending on their design, may need more power than 11a/g units. This may mean new PoE switches or power bricks. If a vendor says you don't need to upgrade your older PoE to run its 11n gear, challenge it to prove it.



A n a l y t i c s R e p o r t

Ensure that those responsible for end user device provisioning are in the loop; to take advantage of 11n, your client computers must be 11n-capable. All new purchases should feature dual-band Wi-Fi cards so that they can operate in either the 2.4 GHz or 5 GHz spectrum with the number of spatial streams required for your throughput needs. Create a client NIC hardware specification, and plan new purchases accordingly. Retrofit currently owned units where it makes sense.

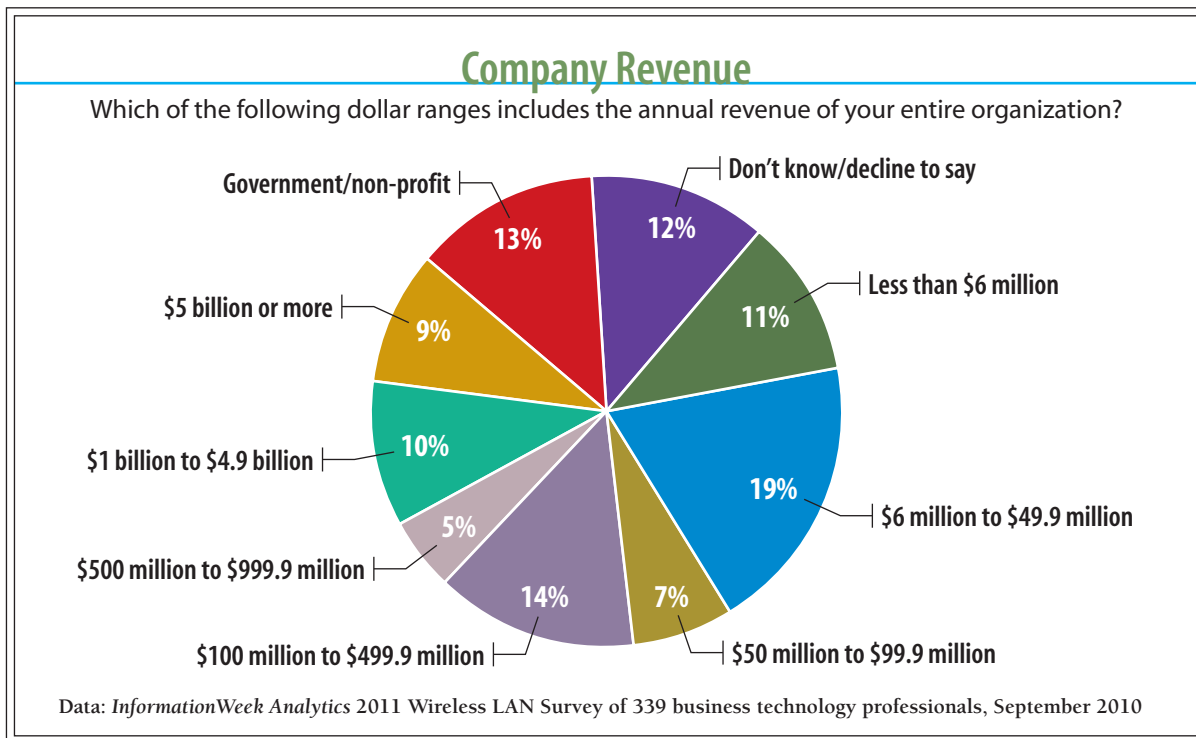
Don't forget regulatory compliance and fitting the WLAN into your security program. Your choice of authentication and encryption or the placement of auditable systems within the WLAN may affect audit results. Thus, be preemptive and follow a data-centric security philosophy to avoid getting flagged.

Use enterprise-grade authentication and encryption. Specifically, employ WPA2 wherever possible along with a strong authentication type that is compatible with your back-end user directory and compliant with your stated security policy and risk profile.

Education is key because WLAN technology is complex. Start with vendor-neutral training, followed by vendor-specific training. This approach will help IT staff understand how WLANs work and give them the knowledge to troubleshoot when necessary.



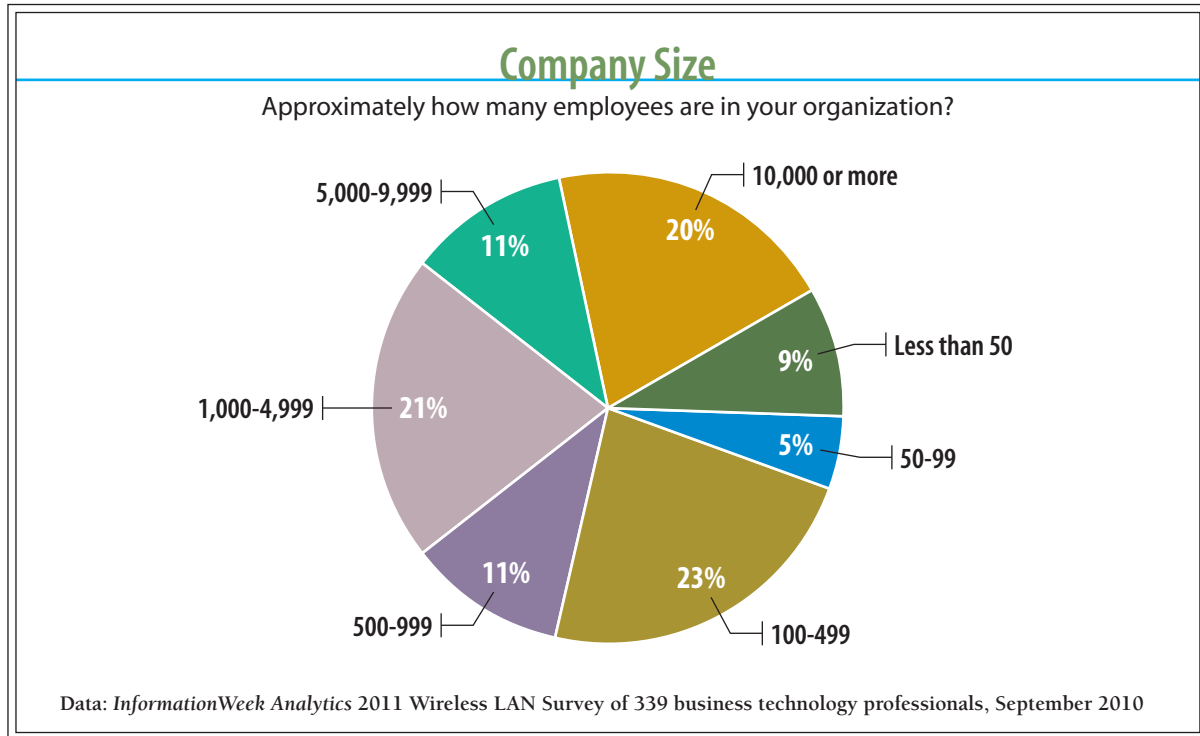
Figure 26





Analytics Report

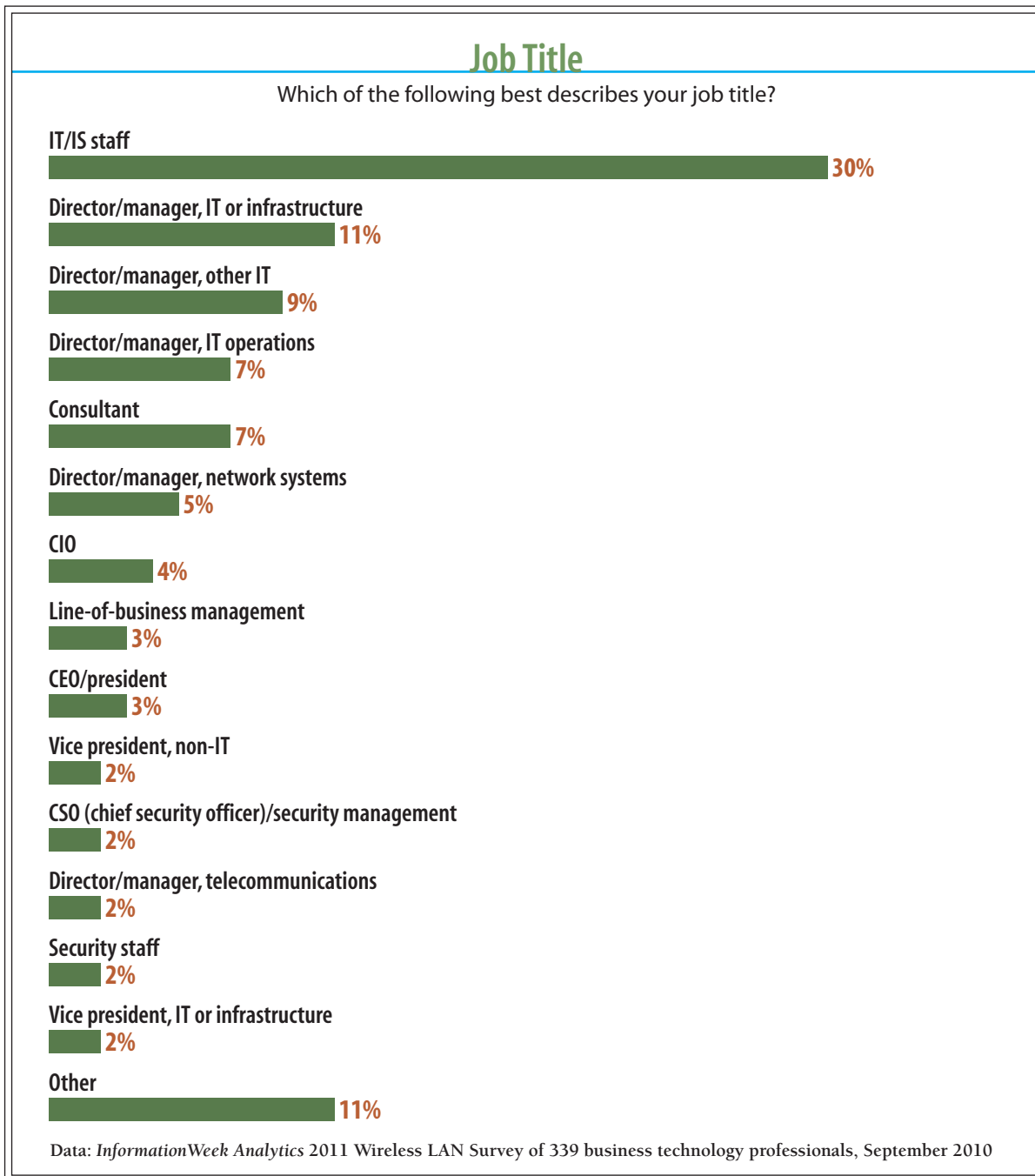
Figure 27





Analytics Report

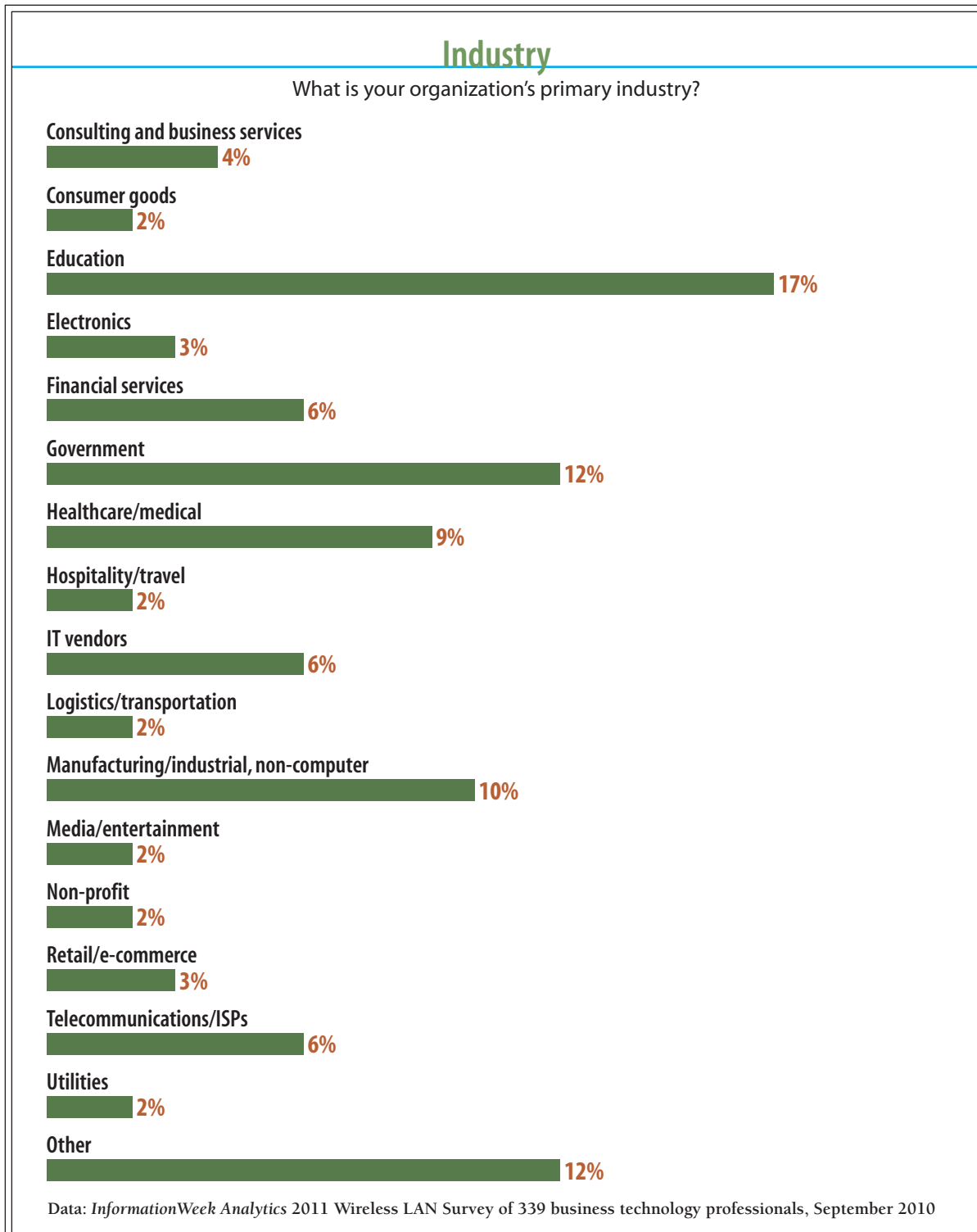
Figure 28





Analytics Report

Figure 29





Analytics Report

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying new projects or implementing new systems, there's no substitute for experience. And that's what **InformationWeek Analytics** provides—analysis and advice from IT professionals. Our subscription-based site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2010. **InformationWeek Analytics** members have access to:

Research: Mobile Device Management & Security: When it comes to setting policies for end users' smartphones and other portable gear, since 2008, IT groups have largely gotten away with being on cruise control. No more.

Research: End User 2.0: Employees have never been more demanding about technology. IT needs to treat that as an asset. Our exclusive research looks at how IT teams are working with end users in new ways, and at where they struggle to do so.

Informed CIO: Mobile Management Policies: Given the increasing mobilization of enterprise applications, it's time to put policies in place to ensure proper governance and keep costs under control.

Informed CIO: Mobile Broadband Beyond Smartphones: 3G or Wi-Fi? Should you tether phones to your new devices? And what kind of security is right? Smartphones pack a whole lot of computing power into one little device, so make informed decisions.

Best Practices: WLAN Management: We've come a long way in the past decade, from, "Look Ma! No wires!" to 802.11n networks that promise to eventually deliver 600 Mbps throughput. Here's how to manage through the next transition.

PLUS: Signature reports, such as the *InformationWeek Salary Survey*, *InformationWeek 500* and the annual State of Security report; full issues; and much more.

For more information on our subscription plans, please [CLICK HERE](#)